Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 471-477, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23626

Secure AASR Protocol with Trust for Manets in Adversarial Environment

R. Archana and W. Gracy Theresa

Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India

Abstract: MANETs are deployed in adversarial environment it is important to provide a security based on onion routing mechanism a security is provide by authenticating the route request packet to satisfy unidentifiability and unlinkability, maximizing the throughput. In order to reduce the delay and to evaluate energy consumption the AASR protocol is combined with trust based routing protocol so that the protocol will be more dynamic in detecting the link failure that has been caused by mobility are adversarial attack. Onion routing method and group signature are used. The AASR is improved by combining it with trust based routing protocol so that it will be more active in detecting the link failure. To improve security based on onion routing mechanism and combine the AASR protocol with trust based routing protocol so that it will be more active in detecting the link\ failure caused by competitor attack. Performance, delay throughput, energy consumption, packet count, queue size are the parameters evaluated.

Key words: Unidentifiabilty · Unlinkability · AASR · Trust · Record Based Trust · Onion Routing · Group Signature

INTRODUCTION

MANET is defined as a self-configuring less infrastructure network where mobile devices are connected without wires.Each devices in the MANET is free to move independently in any direction and in therefore change its link to any other devices frequently. They do not need have any fixed infrastructure to be configured which makes it more suitable to be used in environments that require on the fly setup. In MANET it is difficult to provide trusted and secure communications in competitor nature, such as battlefields. The competitors outside a network may infer the information about the articulating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. On the other hand, the nodes inside the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. As a result, shadowy and trust based articulation are important for MANETs in competitor nature, In order to provide the trust based articulation the onion routing mechanism is combined with trust based routing technique which gathers the neighbor node information such as energy, packet count, queue size for identifying whether the node is trust are not by calculating the computer threshold value.If the value is greater than the targeted value then the node is considered as a malicious nodes and the node will be added to the block list. And for route discovery the key-encrypted onion mechanism is used to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage and the Group signature is used to authenticate the RREQ packet per jump, to counteract intermediate nodes from modifying the routing packet.

Secure Distributed Anonymous Routing Protocol: Secure Distributed Anonymous Routing Protocol [13] has been proposed to provide security, anonymity and high reliability of the established route in a hostile environment such as ad hoc wireless network by using the neighbor discovery scheme, which is used to identify the neighbors [2] in the communication range. The major objective of this protocol is to allow trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes.

Corresponding Author: R. Archana, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur India.

Anonymous Dynamic Source Routing: Anonymous Dynamic Source Routing for Mobile Ad Hoc Networks4 have been proposed based on the analysis to provide three levels of security protection such as Security, anonymity and scalability. This protocol uses cryptographic mechanism that is Diffie Hellmann key agreement to create a shared session key [9] for a security communication between the source node and destination node.

Mask: MASK [5] is a novel anonymous on demand routing protocol, This protocol have been proposed to enable both anonymous MAC layer and network-layer communications so as to thwart adversarial, passive eavesdropping and various types of attacks by using Pairing Based Cryptography. MASK provides the anonymity of sender's relationships, receiver's relationships and sender-receiver relationships, as well as node unlocalability and untrackability and end-to-end flow untraceability [7].

Anonymous Routing Protocol for Mobile Ad Hoc Networks: Stefaan Seys *et al*. [l8] presents a mysterious on interest directing plan for MANETs where the source and the destination share a mystery key KSD and a mystery pen name. The source will incorporate this pen name the course asks for message [10]. The destination will have a rundown of nom de plume by various sources in its memory and it confirms whether the message is focused at it or not.

This alias utilized once (for a solitary course ask for message). The destination sends the answer with the same nom de plume [6]. On the receipt of the answer message source begins to send the information alongside the onetime identifier appended with them. One time identifier shields the information from the aggressor.

Trust-Based on-Demand Multipath Routing in Mobile Ad Hoc Networks: X. Li, Z. Jia, P. Zhang, R. Zhang and H. Wang [11] here, trust of a node is represented as a weighted sum of forwarding ratio and path trust is computed as a continued product of node trusts. Here, the node is considered as malicious based on its forwarding behavior. Misbehaving nodes may participate in the Route Discovery but may refuse to forward the data packets.

Faces: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems: K. Verma, K.Geetha [12,13] trust of the nodes is determined by sending challenges and sharing friends' lists. The proposed algorithm is divided into four stages: Challenge your neighbor, Rate friends, Share friends and Route through friends. Challenges are sent to authenticate the nodes. Nodes which complete the challenge are put into the friend list and otherwise they are put into the question mark list. In rate friends stage friends rating is done on the basis of the amount of data they transmit and rating obtained by other friends.

Multi-Path and Message Trust-Based Secure Routing in Ad Hoc Network: S.K. Dhurandher and V. Mehra [14] proposed a trust based routing which protects the message against alteration. In this, trust is calculated in an active way and less trusted path may also be used to transmit data depending upon the security requirement of the message

Security in Mobile Ad-Hoc Networks Using Soft Encryption and Trust Based Multipath Routing: P. Narula, S. K. Dhurandher, S. Misra and I. Woungang [15], it uses soft encryption techniques in which the message is divided into parts and the parts are self-encrypted. The number of encrypted parts of a message given to a node for forwarding depends upon the trust value of that node.

MATERIALS AND METHODS

The following details explains how the encryption and decryption process takes place to discover a route

Anonymous Route Request

Source Node: Assume that S initially knows the information about D, including its pseudonym, public key and destination string. The destination string dest is a binary string, which means "You are the destination" and can be recognized by D. If there is no session key, S will generate a new session key KSD for the association between S and D.

S → *: [RREQ,Nsq,VD,VSD,Onion(S)]GS

Where RREQ is the packet type identifier; Nsq is a sequence number randomly generated by S for this

route request; VD is an encrypted message for the request validation at the destination node; VSD is an encrypted message for the route validation at the intermediate nodes; Onion(S) is a key encrypted onion created by S. The whole RREQ packet is finally signed by S with its group private key GS. After sending the RREQ, S creates a new entry in its routing table

Intermediate Node: The RREQ packet from S is flooded in T. Now we focus on an intermediate node I, we assume that I have already established the neighbor relationship with S and J. I know where the RREQ packet comes from. Once I receives the RREQ packet, it will verify the packet with its group public key GT+. As long as the packet is signed by a valid node, I can obtain the packet information. Otherwise, such an RREQ packet will be marked as malicious and dropped. Then I try to decrypt the part of VD with its own private key. In case of decryption failure, I understand that it is not the destination of the RREQ. I will assemble and broadcast another RREQ packet in the following format:

I→ *: [RREQ,Nsq,VD,VSD,Onion(I)]GI

Where Nsq, VD and VSD are kept the same as the received RREQ packet; the key-encrypted onion part is updated to Onion (I). The complete packet is signed by I with its group private key GI-.

Onion (I) = OKSI (NI,Onion(S))

Destination Node: When the RREQ packet reaches D, D validates it similarly to the intermediate nodes I or J. Since D can decrypt the part of VD, it understands that it is the destination of the RREQ. D can obtain the session key KSD, the validation nonce Nv and the validation key Kv. Then D is ready to assemble an RREP packet to reply the S's route request.

Anonymous Route Reply

Destination Node: When D receives the RREQ from its neighbor J, it will assemble an RREP packet and send it back to J. The format of the RREP packet is defined as follow:

D → *: (RREP,Nrt,Kv,Onion(J)KJD)

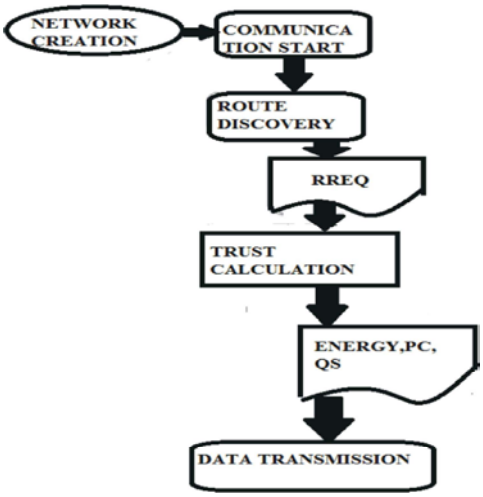
Intermediate Node: We assume that J has already established a neighbor relationship with I, D and M. When the RREP packet travels according to the layers on the onion, it will start at the destination node and move back to its previous node. Each time the intermediate node can associate a value with the underlying wireless link on which the RREP travels, until the RREP packet reaches the source. In our protocol, every node records the one-time link pseudonyms announced by its neighbor node. Then the intermediate nodes' forwarding tables can be established after the RREP's trip.

Source Node: When the RREP packet reaches S, S validates the packet in a similar process to the intermediate nodes. If the decrypted onion core NS equals to one of S's issued nonce, S is the original RREQ source. Then the route discovery process ends successfully. S is ready to transmit a data along the route indicated by Nrt.

Routing Procedure:

- During route discovery, a source node broadcasts an RREQ packet[1].
- If an intermediate node receives the Route Request packet, it verifies the Route Request packet by using its gathering open key and adds one layer on top of the key-encrypted onion. This process is repeated until the Route Request packet reaches the destination or expired.
- Once the RREQ is received by the destination it verifies the Route Request packet and it responses the source node by broadcasting the Route Response packet.
- When the destination node broadcast thee Route Response packet through the intermediate node, each intermediate node validates the RREP packet and updates its routing and forwarding tables. Then it removes one layer on the top of the encrypted Key and continues broadcasting the updated RREP.
- When the source node receives the RREP packet, it verifies the packet and updates its routing and forwarding tables. The route discovery phase is completed.
- The source node starts data transmissions in the established route. Every intermediate node forwards the data packets by using the route pseudonym.

Improving AASR Protocol



Trust based authenticated anonymous secure routing protocol has been proposed by Improving AASR by combining it with the trust based routing protocol. Based on the onion routing mechanism the route is discovered and for trust calculation the record and trust based algorithm is used. After discovering the route the trust calculation is done. The Trust based security in mobile ad hoc network uses record based trust algorithm to gather the neighbor node information such as energy, packet count, queue size and identifies whether the node is trust or not. C_TV (Computer threshold value) value is calculated.If the value is greater than the targeted value then the nodes is consider as a malicious node and that node will be added to the block list. If the value is lesser then the threshold value then the data will be transmitted. And then the performance analysis is done. By using the proposed system the end to end delay is reduced and provides high anonymity by doing this the network lifetime is extended at lower cost.

Record Based Trust Algorithm

Route discovery process start
Neighbor node information gathered
i) Energy
ii) Packet count
iii) Queue Size
Trust calculation

$$Tc = (ts + P / 2)/t+p$$

Where,
Tc -Trust calculation
ts -time success
P-Positive real number
t-Time transaction
The current trust value is retrieved.
    if (T_CV > 0.7)
Begin
    Malicious node is detected
    Add to block list
    Else
Data transmitted

RESULTS AND DISCUSSIONS

The Figure 2 shows how the source node sends the route request packet to the intermediate node. The Figure 3 represents key-encrypted onion in order to protect the anonymity when exchanging the route information Onion routing method and Group signature is used. The Figure 4 represents the malicious node detection when the routing information is exchanged from source to destination. The node is marked in red color when it is verified by using the group signature which denotes the malicious node.

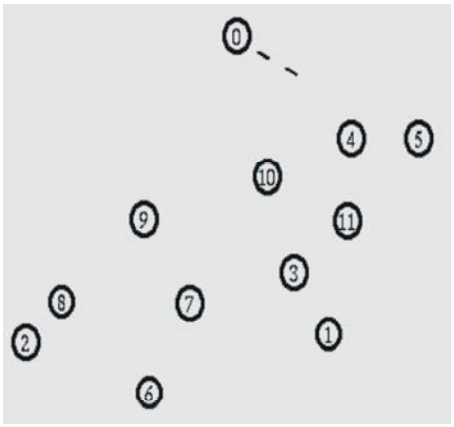


Fig. 2: Anonymous Route Request

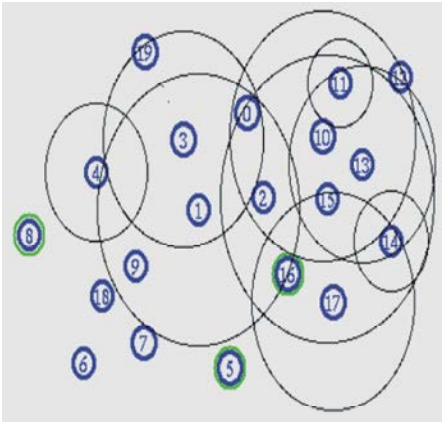


Fig. 3: key-Encrypted Onion

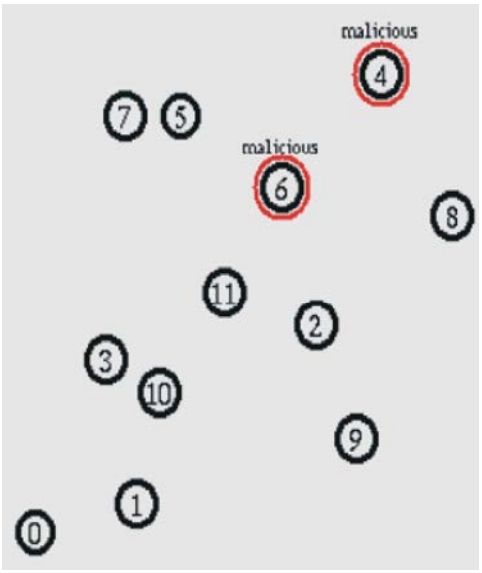


Fig. 4: Malicious Node Detection

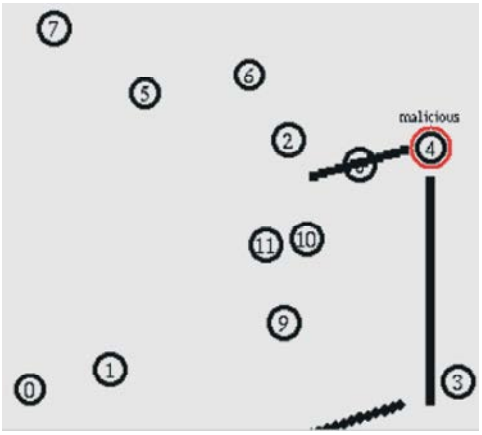


Fig. 5: Packet Dropping

Fig. 6: Adding to Block List

The Figure 5 represents the packet dropped from the malicious node, when the packets are routed through the malicious node 4. Figure 6 shows how the trust is calculated.After discovering the route the trust calculation is done. The Trust based security in mobile ad hoc network uses record based trust algorithm to gather the neighbor node information such as energy, packet count, queue size and identifies whether the node is trust or not. C_TV (Computer threshold value) value is calculated.If the value is greater than the targeted value then the nodes is consider as a malicious node and that node will be added to the block list. If the value is lesser then the threshold value then the data will be transmitted.

Performance Analysis: The Figure 7 represents the performance analysis for the throughput between the two protocols ANODV and AASR. So it is found that the average throughput of ANODV decreases obviously

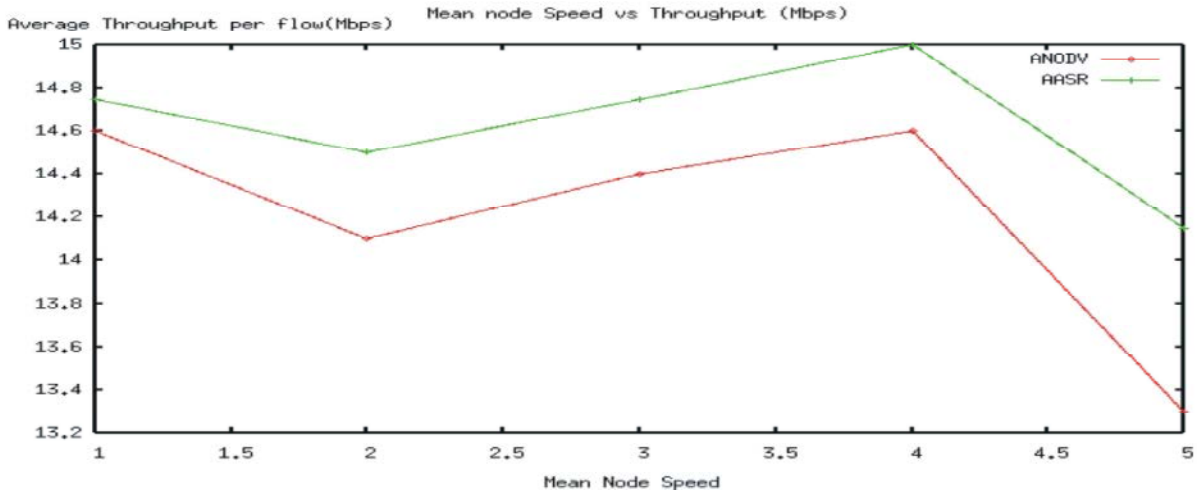


Fig. 7: Throughputs

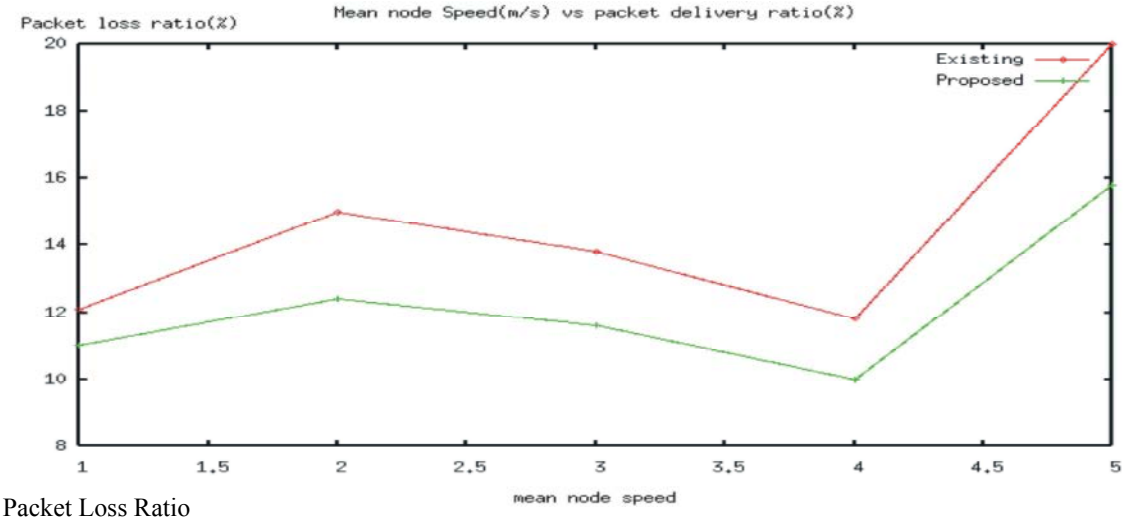


Fig. 8: Packet Loss Ratio

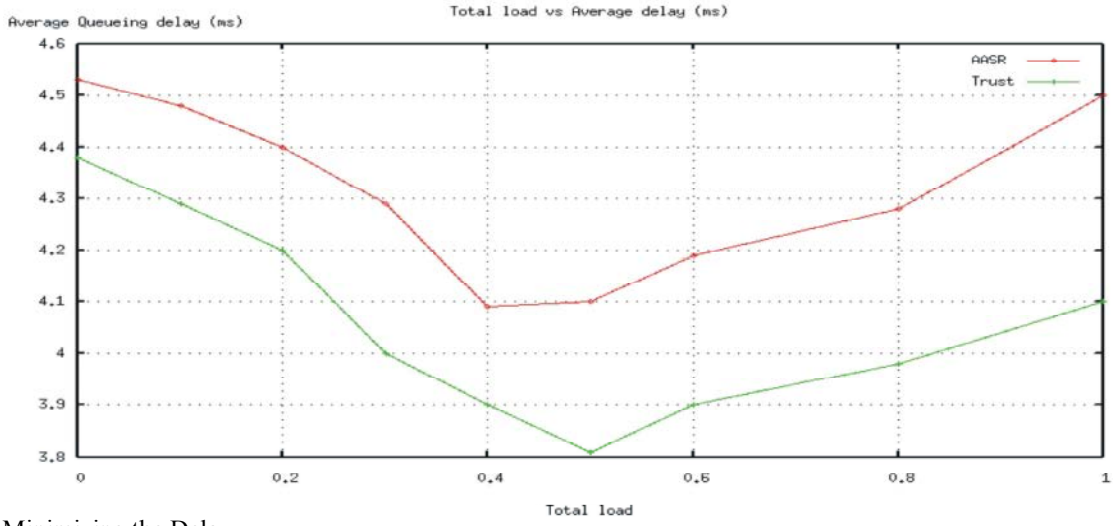


Fig. 9: Minimizing the Delay

when compared to the AASR protocol. In this Figure 8 the existing protocol ANODV is compared with the AASR protocol for the packet delivery ratio and found that the ANODV protocol has higher packet loss ratio then AASR protocol. Figure 9 shows the difference of delay between the existing protocol and the proposed protocol.

CONCLUSION

The AASR protocol is improved by combining it with the trust based routing protocol so that the protocol will be more active in detecting the link failure that have been caused by adversary attack to reduce the delay and to evaluate the energy consumption. The onion routing method is used to increase the throughput and reduce the packet delivery ratio in order to reduce the delay the AASR protocol is combined with the trust based routing protocol. the anonymous route is discovered using onion routing and the trust value is calculated based on record based trust algorithm after calculating the trust value it is compared with the threshold value if the trust value is greater than the threshold value then it is decided that malicious node is present and that malicious nodes are added to the block list. After adding the malicious nodes to the block list the data is transmitted.

REFERENCES

1. Wei Liu and Ming Yu, 2014. AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments, IEEE Transactions on Vehicular Technology, Volume: Issue: 99, Date of Publication,

2. Kong, J. and X. Hong, 2003. ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks, in Proc. ACM Mobi Hoc., pp: 291-302.
3. Boukerche, A., K. El-Khatib, L. Xu and L. Korba, 2004. SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks, in Proc. IEEE Int. Conf. LCN, pp: 618-624.
4. Song, R., L. Korba and G. Yee, 2005. Anon DSR: Efficient anonymous dynamic source routing for mobile ad hoc networks, in Proc. ACM Workshop SASN, pp: 33-42.
5. Zhang, Y., W. Liu, W. Lou and Y.G. Fang, 2006. MASK: Anonymous on-demand routing in mobile ad hoc networks, IEEE Trans. Wireless Commun., 5(9): 2376-2386.
6. Yang, L., M. Jakobsson and S. Wetzel, 2006. Discount anonymous on demand routing for mobile ad hoc networks, in Proc. Int. Conf. SECURECOMM, pp: 1-10.
7. Defrawy, K.E. and G. Tsudik, 2011. ALARM: Anonymous location-aided routing in suspicious MANETs, IEEE Trans. Mobile Comput., 10(9): 1345-1358.
8. Seys, S. and B. Preneel, 2009. ARM: Anonymous routing protocol for mobile ad hoc networks, Int. J. Wireless Mobile Comput., 3(3): 145-155.
9. Wu, X. and B. Bhargava, 2005. AO2P: Ad hoc on-demand position-based private routing protocol, IEEE Trans. Mobile Comput., 4(4): 335-348.
10. Shen, H. and L. Zhao, 2013. ALERT: An anonymous location-based efficient routing protocol in MANETs, IEEE Trans. Mobile Comput., 12(6): 1079-1093.
11. Narula, P., S.K. Dhurandher, S. Misra and I. Woungang, 2008. Security in mobile ad-hoc networks using soft encryption and trust based multipath routing, Sci. Direct Comput. Commun., 31: 760-769, 2008.
12. Dr. Thangaraj, P. and K. Geetha, 2015. An Enhanced Associativity Based Routing with Fuzzy Based Trust to Mitigate Network Attacks, World Academy of Science, Engineering and Technology, 9(8): 1614 1622.
13. Dhurandher, S.K. and V. Mehra, 2009. Multi-path and message trust-based secure routing in ad hoc networks, in Proc. Int. Conf. Advances in Computing, Control and Telecomm.Technologies, pp: 189-194.
14. Dhurandher, S.K., M.S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, 2011. FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems, Systems Journal, IEEE, 5(2): 176-188.
15. Madhusudhanan, B., S. Chitra and C. Rajan, 2015. Mobility Based Key Management Technique for Multicast Security in Mobile Ad Hoc Networks. The Scientific World Journal, 2015. Volume 2015, Article ID 801632, 10 pages http://dx.doi.org/10.1155/2015/801632
16. Li, X., Z. Jia, P. Zhang, R. Zhang and H. Wang, 2010. Trust-based on-demand multipath routing in mobile ad hoc networks, Information Security, IET, 4(4): 212-232.