ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

A REVIEW ON SECURITY ENHANCEMENT THROUGH ANONYMOUS ROUTING IN MOBILE AD HOC NETWORK

DRISHYA SR, VAIDEHI VIJAYAKUMAR

Department of SCSE, School of Computer Science Engineering, VIT University, Chennai, Tamil Nadu, India. Email: Sr.drishya@gmail.com

Received: 03 March 2017, Revised and Accepted: 05 March 2017

ABSTRACT

Mobile ad hoc network (MANET) is an infrastructure less network. Any node may enter or leave network at anytime. MANET also has less resources and limited security. MANET is vulnerable to attacks because of its lack of centralized infrastructure. Security in MANET can be achieved by anonymous routing which hide source, destination and route information to provide. This paper provides a review on efficient anonymous routing protocols used in MANET and also compares the security in terms of identity, location, and route anonymity. An anonymous routing protocol that conceals the essential details and satisfies the basic protocol properties has to be proposed.

Keywords: Anonymity, Privacy, Data security, Mobile ad hoc networks, Location-aided routing.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19629

INTRODUCTION

Compared to wired networks, wireless networks are more vulnerable to several attacks. This is due to dynamic nature, open medium, and lack of centralized management. One among them is mobile ad hoc networks (MANET). In this network, a node acts as both source and router. It can join or leave the network at anytime. MANET is very useful in military applications because of its adaptability and self-organizing capability [1]. Current research work in MANET concentrates on providing authentication, confidentiality, availability, and fairness. And now recently anonymity is also added to the research.

Traffic analysis is the major problem in MANET. By observing the traffic in MANET, attackers can get vital information regarding the network. For example, an attacker can identify the location of communication parties by observing traffic which leads to severe threats in the network [1,2]. In battlefield ensuring attackers cannot disclose our communication information is not sufficient the identity should be closed and location of the communication parties. In such cases, anonymous communication is needed [3].

Anonymity [4] is the important feature that can be provided to the network, especially in vital environments like military. To avoid possible traffic analysis, pseudonyms are used instead of identifiers in routing to hide the identity of the nodes [5,6]. Attackers cannot correlate the original identity of the node with pseudonyms as they change frequently with a certain time limit.

To provide the security to data communication between source and destination, cryptographic schemes are used. This results in development of "Onion scheme" [7] in routing in route discovery phase as it already used for internet anonymous data transmission. As nodes are moved in the network there may be loss or break in the path, to avoid this problem on demand anonymous routing is proposed [8].

Rest of the paper is organized as follows. Section 2 discusses the available anonymous routing protocols for MANET. Section 3 provides the comparison of protocols and conclusion is given in Section 4.

ANONYMOUS ROUTING PROTOCOLS IN MANET

This section analyzes some anonymous routing protocols used in MANET. The protocols can be classified based on the types of networks - flat networks and hierarchical networks. However, this paper mainly focuses on different types of flat network anonymous routing protocols (Fig. 1).

Anonymous on demand routing (ANODR)

ANODR [7] has three phases of anonymity route discovery, route maintenance, and route forwarding. Source initiates the communication by broadcasting RREQ packets to the remaining nodes in the network. ANODR is identity-free except in its first route discovery. It does not incur any public encryption overhead in RREQ flood. Source generate a random number as onion core. Each forward node of RREQ adds a layer of encryption and it can be peeling off by only that node during RREP phase. Onion structure is formed during RREQ phase, and during RREP phase it can be turned to anonymous virtual circuits. ANODR implements destination-initiated RREP procedure. It uses symmetric key agreement for RREP. It possesses global trapdoor that stores secret information about the destination and its public key (Fig. 2).

For route maintenance, ANODR recycles the routing table entries on time limit. When one or more nodes left the network, then a node cannot send a packet to intended destination. Source can find these types of anonymities when retransmission requests exceed the threshold value.

Anonymous dynamic source routing (AnonDSR)

AnonDSR [9] has two phases of anonymity route discovery and data transfer. Anonymity route discovery protocol establishes route between source and destination. Source and destination uses this protocol when they share a secret key. Anonymous data transfer protocol establishes a cryptographic mechanism for anonymous data protection in the communication. This establishes a cryptographic onion at each node during RREQ phase. Each intermediate node has to check the pseudonym of the packet. If the data packet belongs to it, then it decrypts the data onion layer using its session key. Node changes the route pseudonym while forwarding a packet using decrypted onion. Then, it broadcast the new packet. This procedure repeats until data packet reaches the intended destination.

In route request phase, source node creates packet "<ANON-RREQ, PK_{temp}, tr_{dest}, onion>" and then broadcast it where PK_{temp} is temporary public key and also works as a unique sequence number and tr_{dest} is trapdoor that can be only opened by destination with shared secret key. For building an anonymous communication channel, a session

key K_X is shared among intermediate nodes. N_X is a local pseudonym, N_K' is the new key index and K' is shared secret key used to update the old key and secret keys N_K and K for the next communication, and $SignA = ESKA\ (H(PK_{temp}, SK_{temp}, K_A, ID_A, ID_E, PK_A, N_K, K, N_K', K', PL, P))$ (Fig. 3).

In route reply phase, destination decrypts the onion using private key obtained from trapdoor and verifies if all data are correct. With anonymous route pseudonyms and session keys destination creates a path reverse onion.

$$PRO_D = E_{K_D}(N_C, E_{K_C}(N_B, E_{K_B}(N_A, E_{K_A}(N_B, K_B, N_C, K_C, N_D, K_D, PL, P, Sign_E)))),$$

It then adds a route $< N_D, K_D, N_A, K_A, N_B, K_B, N_C, K_C >$ into its routing table. It uses the N_D as anonymous route pseudonym for this communication. Then, the destination node creates ANON-RREP packet and broadcasts the packet locally $<ANON\text{-}RREP, N_D, PRO_D>$.

After receiving the ANON-RREP packet, all intermediate nodes check whether N_D is in their pseudonym or not. If N_D is not pseudonym, then the node will discard the packets. With the help of session key K_D, Node D decrypts the layer of the onion PRO_D with respect to the pseudonym N_D and gets N_C and PRO_C. This continues until it reaches to source node A (Fig. 4).

MASK

The basic idea of MASK [10] is (1) anonymous neighbor node authentication with dynamically changing pseudonyms of nodes and (2) route discovery and data forward can be done by pair wise shared link id between neighbor nodes. The objective of MASK is: Anonymity of sender, receiver and communication, unlocatability and intractability, secure neighbor authentication, high routing efficiency, and low cryptographic overhead. MASK uses proactive neighborhood detection protocol. Each node knows the physical existence of the neighbor node but not their identity. For providing communication two nodes should agree prior. For this MASK uses three-way handshaking. Any node

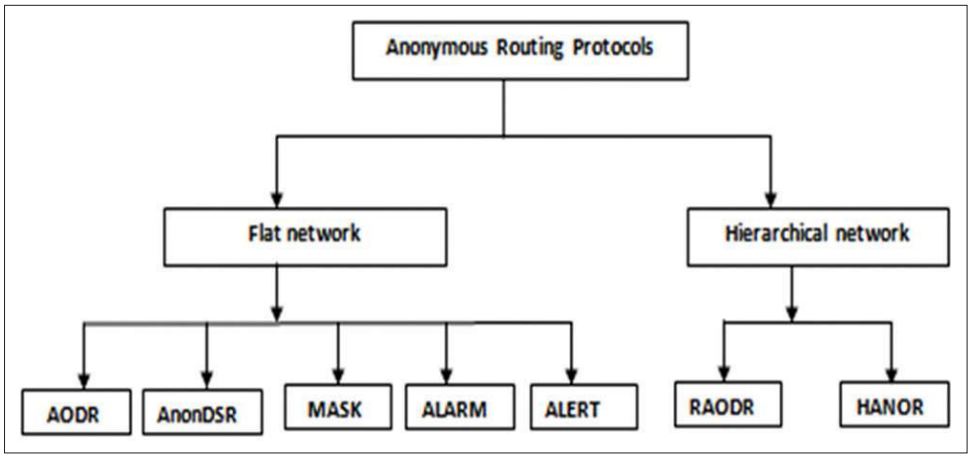

Fig.1: Classification of anonymous routing protocols in mobile ad hoc network

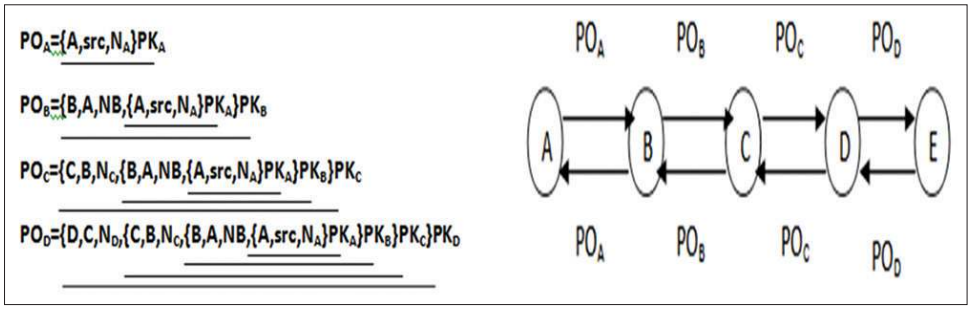

Fig. 2: Anonymous route discovery using public key cryptography

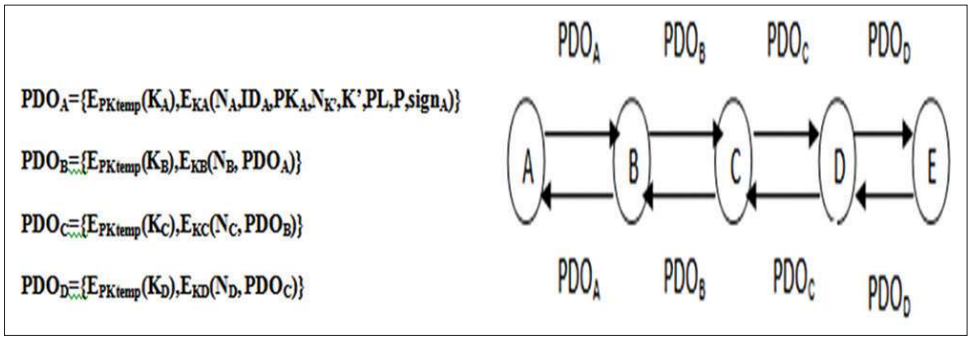

Fig. 3: Anonymous dynamic source routing protected path discovery onion

wants to communicate it send the request to neighbor node. Instead of sending it id along with the request, it send pseudonym. If the neighbor node also willing to communicate then it sends it replies along with its pseudonym. Then, these nodes agree to a shared key and link id and then communicate with each other (Fig. 5).

If any one of the nodes is illegitimate, then no information is revealed except pseudonym of the node. With the help of pseudonym attacker cannot get any information. However, this pseudonym should be changed frequently. MASK does not use any global trapdoor. Source put RREQ packet explicitly in destination node id. This reduces the overhead of communication. However, the difference to traditional routing and in MASK is every node need to rebroadcast the RREQ once including destination node.

Anonymous location aided routing (ALARM)

ALARM [11] is a secure link state and privacy preserving algorithm. Pseudonyms are created with group signatures. With this group signature technique it can provide node authentication, data integrity, and anonymity. A group manager (GM) is assigned to identify the nodes having group signatures. GM starts group signature scheme. It generates the private key for all the group members. A public key is created by all nodes and reveal it to only GM. Time is divided into slots. Every node selects a public-private key pair at the beginning of each time slot. Location announcement message (LAM) contains all the information regarding location, group signature, public key, and time stamp. This LAM is broadcasted to the network. When a node receives LAM, first it checks whether it receives it for the first time or already received. If it receives it for the first time, then it authenticates the group signature and time stamp. If the LAM is valid, then it broadcasts again and collects each node LAM. With this information, connectivity and geographical graphs can be maintained. When a node has to communicate to another node in some location, first it has to check whether node is available in that location. If a node is available in that location, then temporary id for the destination should be obtained by sending a message to that node. To encrypt the data session key is used and this session key is encrypted with public key. When receiver receives the message it should decrypt the session key with public key and then the message.

Anonymous location-based efficient routing protocol (ALERT)

ALERT [12] uses hierarchical partition technique to reduce encryption cost and traffic overhead. It partitions the network dynamically into vertical and horizontal zones.

For data transmission it uses greedy perimeter stateless routing. ALERT restrict the visibility of the node to its neighbor. At every node, initial and forward messages are created so that attacker cannot know

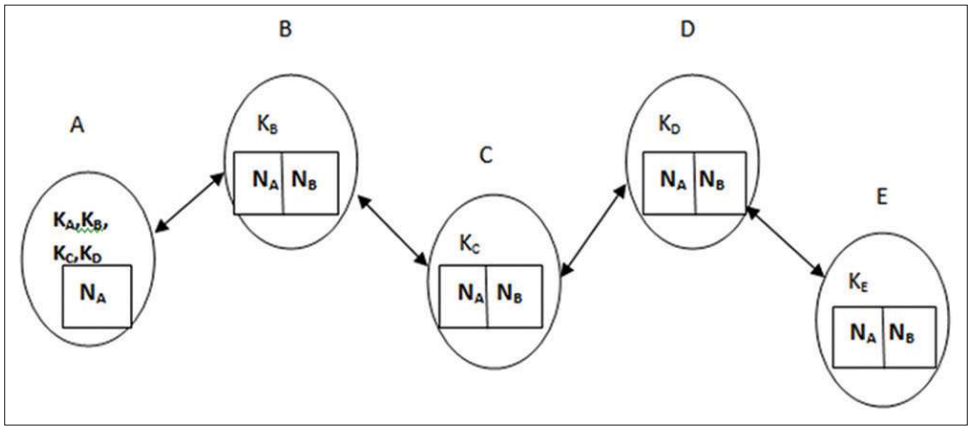

Fig. 4: Anonymous dynamic source routing anonymous route

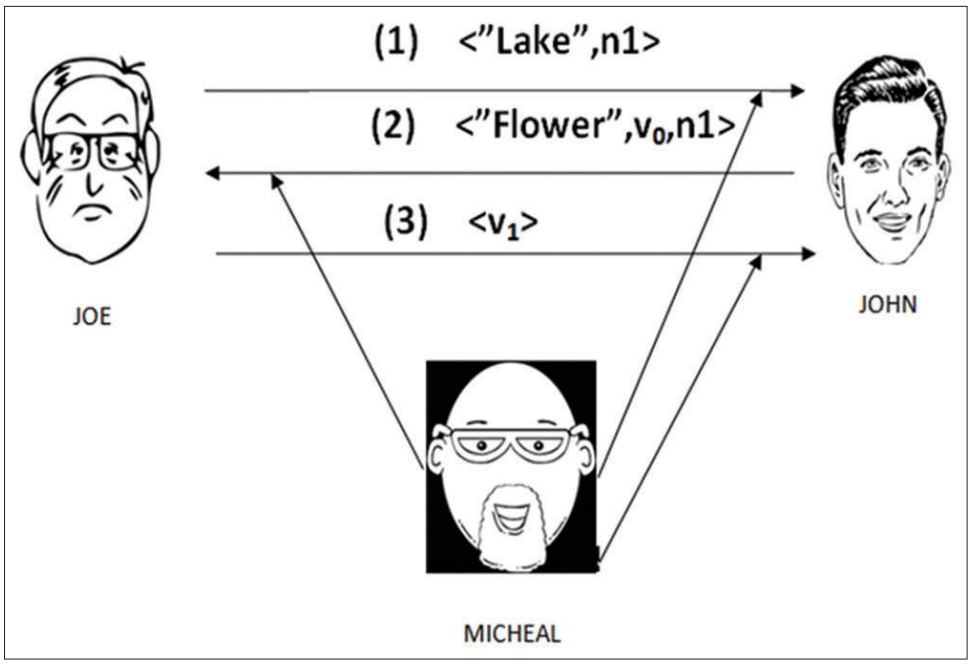

Fig. 5: Anonymous neighborhood authentication

whether a node is a source or forwarded node. Another mechanism used is "notify and go." Whenever source sends data, simultaneously many numbers of nodes send the data to hide source node from all the nodes. Likewise, at destination node, many nodes are present to hide destination. Nodes at the destination zone depend on the density of the network (Fig. 6).

COMPARISON OF DIFFERENT ANONYMOUS ROUTING PROTOCOLS

Comparison of the protocols done based on the anonymity parameters. An efficient anonymous protocol should provide anonymity to the MANET under any circumstances. However, the available protocols have restrictions in providing anonymity [13].

ANODR protocol is purely on demand routing protocol. It does not use any public key cryptography to reduce overhead. It also uses global trapdoor to secure the location of destination. It also provides anonymity to data also. However, it lacks in providing route anonymity through which attacker can find the sensitive information about the MANET.

AnonDSR protocol is extension to DSR protocol. It is also purely on demand routing protocol. This protocol uses onion core in routing which results in encryption at each forwarding node and also decryption at RREP phase. This leads to traffic overhead in the network. And also public key cryptography uses large keys and more number of CPU cycles which also leads to computation and communication overhead.

MASK is a proactive routing protocol. It provides low cryptography overhead and efficient routing. It implements proactive neighbor node detection to get the view of neighbor routes. But in incurs both communication and computation overhead at each and every node.

ALARM uses node location to provide security and also to construct a topology view. By implementing advanced cryptographic techniques it can able to provide both security and privacy. It provides authentication, anonymity, data integrity, and resistance to tracking. However, it fails to provide full security for both source and destination location anonymity.

ALERT [14,15] partition network into zones and randomly chooses nodes from different zones as intermediate nodes. This provides route anonymity. In data forwarding mechanism also data sends to multiple nodes along with destination to provide k-anonymity to the destination node. For source node also notify and go mechanism is used to provide anonymity. However, the major drawback in ALERT protocol it increases the traffic overhead by providing anonymity to both destination and source. Data are forwarded to more number of nodes and also whenever sender is sending data, a few other nodes also sends data to hide sender which always lead to more traffic in the MANET (Table 1).

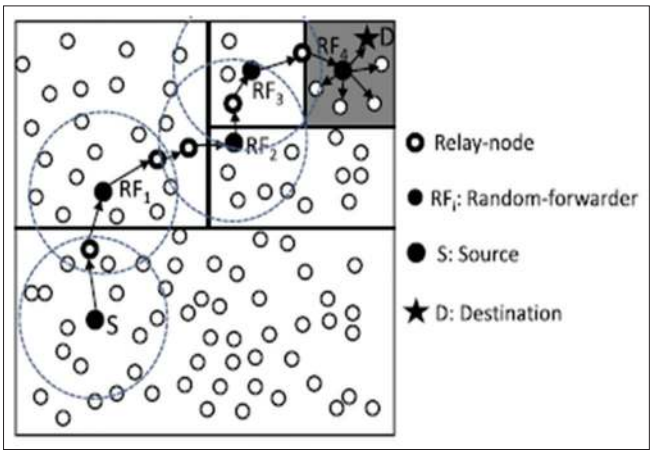

Fig. 6: Routing among zones in anonymous location-based efficient routing protocol

SCOPE FOR FUTURE ENHANCEMENT

Many anonymous routing protocols developed might concentrate on the quality of service (QoS) and security. But achieving these parameters will result in routing overhead. Hence, an optimal protocol should be developed. The protocol should be developed such that it can able to provide secure data transmission and at the same time it should not affect QoS. The data should be encrypted while transmission to avoid eavesdropping attack but it cannot affect cost of routing. One such approach is dividing the network into clusters. Communicate RSA algorithm for data encryption to all nodes. Data encryption can be done at group level, and a group id is maintained to provide anonymity, and at the same time, a method can be invoked that verifies the data sent by intermediate nodes in the cluster. Through this node, anonymity can be provided. However, we have to enhance to provide node, route, and location anonymity (Fig. 7).

The optimal anonymous routing protocol should provide both QoS and cost-effectiveness. Anonymity should be provided to the node in the network to hide node information in an effective way. Finding a path from source to destination using on demand routing to be done. Data should be encrypted in transmission to avoid eavesdropping attack. Asymmetric cryptosystems provides efficient security than symmetric, but it involves more computation cost. In MANET a node can enter or leave the network at anytime. So route should be maintained. It involves more computations. Whenever a node leaves or joins again route should be updated and results in routing table updating throughout the route. Hence, it results in more cost. Hence, the protocol should be cost-effective.

CONCLUSION

Anonymity is more important nowadays to provide security to MANET. It allows users to have privacy communication among the network. Many protocols are implemented to provide anonymous communication in the network. Each and every protocol has its own merits and demerits. Each protocol uses different techniques to provide

Table 1: Comparison among all anonymous protocols in the MANET

Protocol	Proactive/ reactive	Identity anonymity	Location anonymity	Route anonymity
ANODR	Reactive	Data packet	Destination	No
AnonDSR	Reactive	Data packet	-	No
MASK	Reactive	Source, destination	Source	No
ALARM	Proactive	Source, destination	Source	No
ALERT	Reactive	Source, destination	Source, destination	Yes

MANET: Mobile ad hoc network, ANODR: Anonymous on demand routing, AnonDSR: Anonymous dynamic source routing, ALARM: Anonymous location aided routing, ALERT: Anonymous location-based efficient routing protocol

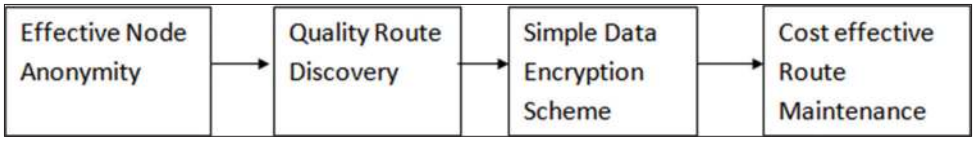

Fig. 7: Optimal anonymous routing protocol

anonymity. Different cryptosystems used in the protocols also result in a difference in efficiency of the protocol. Symmetric cryptosystems have less computation for both encryption and decryption. But asymmetric cryptosystems provide more security than symmetric systems. Among all the protocols discussed in this paper, ALERT is providing more efficient anonymity. However, it is also having some drawbacks. A new protocol has to be designed to reduce the traffic overhead, with low computation and communication cost and providing efficient location and identity anonymity for source, destination, and route, and also for data messages.

REFERENCES

1. Tehrani AH, Shahnaseerc H. Anonymous Communication in MANET's Solutions and Challenges, IEEE International Conference on Wireless Information Technology Systems; 2010.
2. Zhang Y, Liu W, Lou W. Anonymous Communications in Mobile Ad Hoc Networks, Proceeding INFOCOM; 2005.
3. Remya S, Lakshmi KS. SHARP: Secured Hierarchical Anonymous Routing for MANET, International Conference on Computer Communication and Informatics; 2015.
4. Vijayan A, Yamini C. Anonymous Routing Technique in MANET for Secure Transmission, International Conference on Green Computing Communication and Electrical Engineering; 2014.
5. Kumari EH, Kannamal A. Privacy and Security on Anonymous Routing Protocols in MANET Second International Conference on Computer and Electrical Engineering; 2009.
6. Patil P, Marati N. Preventing DOS and MITM Attack in Anonymous Location Based Efficient Routing Protocol in MANET, IEEE International Conference on Engineering and Technology; 2016.
7. Kong J, Hong X. ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks, Proceeding Mobile Ad-Hoc; 2003. p. 291-302.
8. Liu W, Yu M. AASR: Authenticated Anonymous Secure Routing for MANET, IEEE Transaction on Vehicular Technology; 2014.
9. Song R, Korba L, Yee G. AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks, Proceeding ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05); 2005.
10. Zhang Y, Liu W, Lou W, Fang Y. MASK: Anonymous on demand routing in mobile Ad Hoc networks. IEEE Trans Wirel Commun 2006;5(9):2376-86.
11. Tsudik G, El Defrawy K. ALARM: Anonymous location-aided routing in suspicious MANETs. IEEE Trans Mob Comput 2001;10(9):1345-58.
12. Shen H, Zhao L. ALERT: An anonymous location-based efficient routing protocol in MANETs. IEEE Trans Mob Comput 2013;12(6):1079-93.
13. Kong J, Hong X, Sanadidi M, Gerla M. Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing, Proceeding IEEE Symposium. Computers and Communication (ISCC '05); 2005.
14. Khasnikar AK. Anonymity Protection Using ALERT, International Conference of Innovations in Information; 2015.
15. Arya KV, Saxena R. S-ALERT: Secure Anonymous Location Based Efficient Routing Protocol, International Conference on Industrial and Information Systems; 2014.