IIOAB JOURNAL

ARTICLE

AN EFFICIENT TRUST MODEL FOR PUBLIC-KEY AUTHENTICATION AND DETECTING MALICIOUS NODES IN MANET

Kanimozhi Adivel* **and Navamani Thandava Meganathan**

Department of Computer Science and Engineering, Easwari Engineering College, Tamil Nadu, INDIA

ABSTRACT

In Mobile Ad-hoc Networks (MANET), establishing trust among participating nodes is a challenging task due to the fact that these systems are generally operated in highly dynamic and distributed environments. A Pretty Good Privacy (PGP) like trust model considered to be more suitable for MANETs since they do not require access to a trusted authority. Instead, the nodes themselves are allowed to establish trust by certifying each other in a self-organizing way without involving any Trusted Third Party (TTP). Here, we adopt a strategy by using self-certifying ID-based cryptography that allows mobile nodes to determine public-keys of each other from the nodes' identities and their trust levels. And also, an Exclusion Access-control Mechanism based on trust metric evaluation is introduced to detect and isolate the malicious nodes that inject fake trust relations. We have proposed the certificate-less PGP trust model for public key authentication in MANETs. Hence, by improving trust metric in MANETs, trustworthy keys are determined through a given trust path. An exclusion mechanism is introduced to isolate the malicious nodes. Simulation results prove that the trust models and an exclusion access control mechanism provide an accurate malicious node detection and exclusion.

KEY WORDS
Trust model; Authentication; Certificate; MANET; Trust

Published: 30Oct 2016

INTRODUCTION

Infection Mobile Ad hoc Networks (MANET) [5] are self-configured, dynamic networks in which nodes can move freely. It is an infrastructure-less network of mobile nodes and nodes are connected without wires. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. This results in a highly dynamic, autonomous topology.

Trust evaluation metric plays an important role in providing security against malicious nodes in Mobile Ad Hoc Networks [5]. Trust values are generated by analyzing and computing evidence collected from a number of evidence providers. Trust is generally evaluated based on the evidence that shows a trustor's belief on a trustee, observed performance or behaviour of the trustee, and recommendations on the trustee. The proposed model is intended for self-organized MANETs where mobile nodes do not have access to trusted third parties, not even in the bootstrapping phase. In our approach, public-key authentication is self-certified. Nodes need not to store the public keys of each other. These self-certified public keys are reconstructed whenever it is needed and it saves the memory space [5]. Trust metric is introduced which helps the nodes to reconstruct the public key. This work solves the problem of certificate chaining, computational and communication costs overhead. And, the major problem is detecting the malicious nodes which inject fake trust relations. An Exclusion Access-control Mechanism based on trust metric evaluation which was discussed in [7] is introduced to deal with malicious nodes which inject fake trust relations. An exclusion mechanism is introducing a jury node to detect the suspicious node based on the collected evidence from the reputation module. The rest of the paper is organized as follows. Section 2 presents a discussion of related work. Section 3 describes about the proposed work. Section 4 & 5 describes about the security analysis and performance analysis. Section 6 describes about the conclusion work.

RELATED WORKS

Khaled Hamouid et al. [5] have introduced a recommendation based trust metric to deal with malicious nodes and to allow evaluate the trustworthiness of the self-certified public key through a given trust path. A trust graph is defined with two-trust levels which are key-authenticity trust level and node reliability trust level. This can improve the reliability of the public-key authentication. Huanyu Zhao et al. [1] have proposed a methodology of self-certified public-key authentication using a trust architecture which is similar to Pretty Good Privacy (PGP). Here, the nodes themselves issue certificates for each other based on their own trust opinion and maintains a local repository in which it stores a partial certificate chains. This approach imposes extra delay and large amount of traffic for collecting certificates. Ing-Ray Chen et al. [2] have proposed an integrated social and quality-of-service (QoS) trust protocol (called SQTrust). This trust bias is minimized despite the presence of malicious nodes performing slandering attacks. This approach identifies and validates the best trust protocol settings under which trust bias is minimized and application performance is maximized. The node behaviour model is based on persistent attacks. Some of the random, opportunistic, and insidious attacks with fuzzy failure criteria applied to test the resiliency of our trust protocol design has not yet implemented. LeovigildoSánchez-Casado et al [6] have discussed about the malicious node dropping and they introduced the dynamic trust model and the cross-layer approach is based on an analytical model that represents the forwarding process in an ad-hoc network. This technique improves the trust efficiency and also overcome the computational overhead. Have to improve the performance in nodes which exhibits lower activities. Mohammad Taqi Soleimani et al. [9] have proposed

***Corresponding Author**
Email:
kaniihom2808@gmail.com
Tel.: +91 9655433458

a dynamic trust model to defend network against the malicious node. In this approach, initially a node trusts all immediate neighbourhood nodes and then the node updates their trust value based upon the feedback getting from the neighbours. NS-2 simulation results show that the attack is detected successfully with low false positive probability. This approach does not detect all types of attacks that impacts some delay to the network. Mohamed M. E. A. Mahmoud and Xiaodong Lin [8] have proposed E-STAR mechanism which combines the trust system with energy-aware protocol to achieve the efficient trust implementation system without any false acquisitions.

Saju P John et al. [10] have proposed a technique called self organized key management technique coupled with trusted certificate exchange. Due to the certification exchange the storage overhead exists in large scale networks. Shaheena Khatoon et al. [11] have proposed a combined technique of certificate-less key management and threshold cryptography.This scheme proposed an enhanced security attributes for key management in MANET and also eliminates the need for certificate-based public key distribution and the key escrow problem efficiently. In addition to that it completely removed a trusted third party to distribute the public keys, hence increasing the tolerance of the network to compromised nodes and also saving network bandwidth. But the time consumption is somewhat higher. Shuaishuai TAN et al. [12] have proposed a trust based routing mechanism to derive the security threats. In addition, to avoid malicious nodes, a trust based routing algorithm is proposed to select a path with the maximum path trust value among all possible paths. Then extend Optimized Link State Routing (OLSR) by using the proposed trust model and trust based routing algorithm, called Fuzzy Petri Net - Optimized Link State Routing (FPNT-OLSR). Simulation results show that FPNT-OLSR is very effective in establishing secure routes. It also performs better than existing trust based OLSR protocols in terms of packet delivery ratio, average latency and overhead.

Soumyadev Maity et al. [13] have proposed an on-demand public-key management protocol for self-organized MANETs which does not use certificates; it has some problem related with the authenticity of public keys since the keys are generated by nodes themselves and distributed without any authenticity evidence. This scheme does not use any of an explicit or implicit approach to ensure an authenticity of a public-key. Zhang Yong et al. [15] have proposed an on-demand public-key management protocol for self organized MANETs which does not use certificates; it has some problem related with the authenticity of public keys since the keys are generated by nodes themselves and distributed without any authenticity evidence. This scheme does not use any of an explicit or implicit approach to ensure an authenticity of a public-key. By employing identity-based and threshold cryptography, the proposed scheme eliminates the burden of certificates management and can be high level tolerance to node compromise. Zheng Yana et al. [16] have proposed two security schemes of privacy preserving trust evaluation technique to achieve better computational efficiency and greater security. It ensures trust relationships among system entities and enhances system security. But trust evidence collection and process may cause privacy leakage, which makes involved entities reluctant to provide personal evidence that is essential for trust evaluation. The first scheme achieves better computational efficiency, while the second one provides greater security at the expense of a higher computational cost. Both schemes are secure enough but still there is an issue to overcome an internal attack without breaching privacy. Jin-Hee Cho et al. [3] have proposed a composite trust-based public key management to mitigate the security vulnerability. This proposed scheme employs that trust threshold to determine whether trust the other nodes or not. But this approach imposed some low performance. Sudha Chinni et al. [14] have introduced a distributed trust model for certificate revocation. This certificate revocation imposes a traffic delay to collect the certificates. Kanimozhi and Navamani [4] have proposed the certificate-less PGP trust model for public key authentication. However, detailed implementation has not done. In this work, implementation and performance analysis are presented.

The proposed trust establishment approach is similar to PGP-like trust model which was discussed in [5]. In this model, each entity can issue a certificate to other entity it trusts. This trust relationship is supposed to be transitive which allows the nodes to establish indirect trust relations. After reviewing the previous works, it is analyzed that certificate chaining approach incurs more overhead in terms of computation and storage costs. And also, the detection of node which injects fake trust is complicated in existing work. Hence, we have introduced a certificate-less PGP-like trust model for public-key authentication and a new technique for detecting the malicious nodes which inject fake trust relations.

MATERIALS AND METHODS

The basic idea of our approach is implementing certificate-less PGP-like scheme using an Identity based cryptography technique which in turn allows to performs public-key authentication in a self-organized way. An Exclusion Access-control Mechanism based on trust metric evaluation which was discussed in [7] is introduced to monitor the neighbor nodes which are misbehaved and those nodes inject the fake trust relations.

Network Model and Assumptions

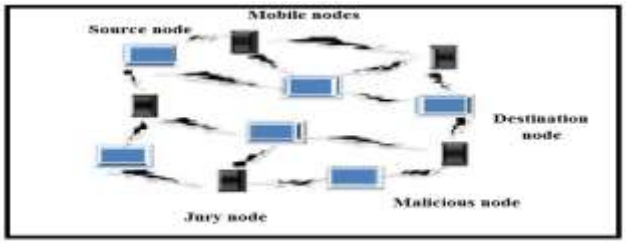

Fig.1: Network model of MANET

.....

[Fig.1] shows the network model of MANET. The proposed network model consists of mobile nodes and jury nodes which are characterized by low capacity in the sense of processing power, storage, energy and bandwidth. Each node can communicate with other nodes via wireless links. Non neighbouring nodes can communicate via multi-hop communications based on ad-hoc routing protocols. The network can change dynamically in the size and topology as nodes can move freely and new nodes can join and others leave at any time without any cost. In this model, it is assumed that each node has a private/public key pair used for authentication and other security purposes. Public keys are self-generated by the node themselves and public keys are cryptographically bound to their owner's identity. The system architecture of the proposed system has source node, destination node and many intermediate nodes. The jury node tracks the information of the neighbouring nodes by monitoring their behaviour. Here, the jury node is used to detect the malicious node whenever it injects fake trust relations.

Notations

The symbols and their description that are used in the proposed scheme are given in the [Table 1].

Table 1: Symbols and notations

Symbols	Description
Wij	Witness generated by node ni to nj
IDj	Unique and public key identifier of node nj
Recij	Recommendation issued by node ni for nj
Tvalij	Trust values between the nodes ni and nj
U	Reputation update unit
Ri-1	Previous reputation value
Rmax	Maximum reputation value
sk	Public key
pk	Private key
hij	Hash function
kij	Prime values

Constructing Trust Model

The proposed trust establishment scheme is similar to PGP model in the sense that users certify each other based on their off-line trust relationships without involving any centralized trusted third party. Khaled Hamouid et al. [7] have introduced a trust model which is defined as two independent trust levels; key-authenticity trust level and node reliability trust level. These trust levels are computed by the neighbouring nodes when it trusts its own neighbouring nodes based on collected evidence.

[Fig. 2] shows the main functions which are happening among the mobility nodes. In our work, four modules are defined such as Constructing trust model, Trust graph establishment & malicious node exclusion, Self-certified key authentication and Key updation. Each node presents in the network having unique id, public-key and private key. While constructing trust level among the nodes, the authenticity of keys and the trustworthiness of the nodes are independent. By these trust levels, a trust graph is formed by issuing witness and recommendations among the nodes. An Exclusion Access-control Mechanism based on trust metric evaluation is introduced to detect and isolate the malicious nodes that inject fake trust relations using jury nodes. Public-keys are reconstructed whenever needed, it saves some memory space. To protect against key disclosure threats, it is better that the nodes should do their periodic

updation of their keys. . Whenever a node leaves the network, it sends a logout request to their trustors and trustees. Whenever a node joins the network, it looks for trustor and trustee nodes.

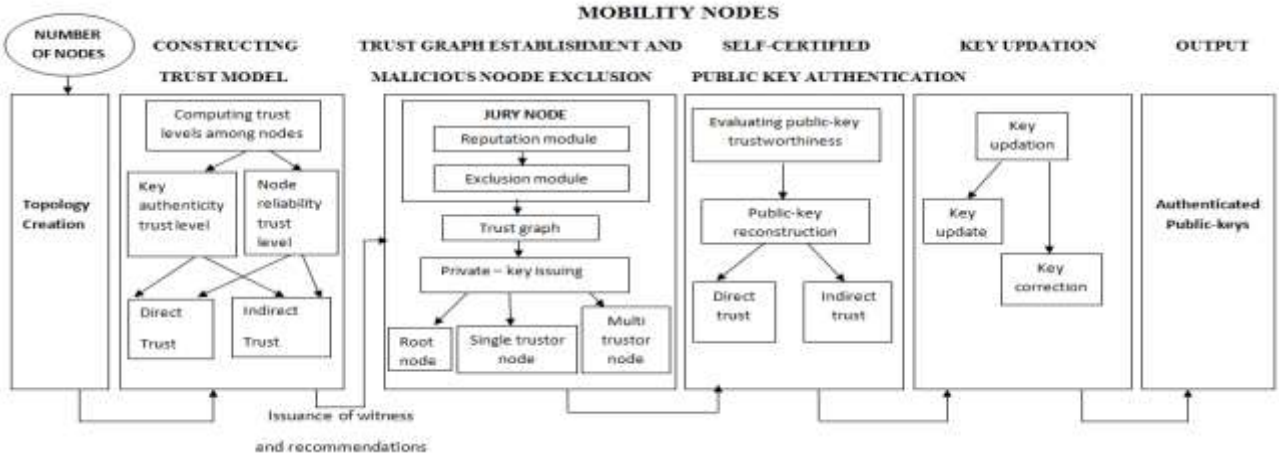

Fig. 2: Functional Architecture

.....

Key Authenticity Trust Level

Key authenticity trust level is that a given node n_i trusts the public-key of another node n_j and should verify its authenticity. Let us assume that the trustor node n_i who trusts a given trustee node n_j. The node n_i issues a witness (W_{ij}) on the n_j's identifier instead of certificates. The issued witness is sent over an authenticated channel to node n_j which uses it to generate the private key. This witness can be viewed as a signature of the issuing node on the ID_j of the node n_j.

Node Reliability Trust Level

It is defined as follows: A node n_i trusts to a certain degree of another node n_j to be reliable for executing the protocol to generate keys to any other nodes. By having this trust level, nodes can issue recommendations and valid witness for any another nodes. An Exclusion Access-control Mechanism based on trust metric which was discussed in [7] is integrated with the proposed system to exclude the misbehaving nodes by the use of accurate and precise trust model which uses past interactions and recommendations to build a trust evaluation in neighbours.

These two trust levels are independent of each other. For example, if a node n_i could not verify the authenticity of another node n_j but still n_i trusts the node n_j and vice versa. This implies that a node is able to evaluate the trustworthiness of another node even it cannot verify the authenticity.

Direct Trust and Indirect Trust Computation

For each trust level, a trust relation among the nodes may be either direct or indirect relationship. Direct trust is represented by a directed edge in the trust graph. If a node n_i has generated a witness to node n_j that can be used to generate its private-key by node n_j, a direct trust relation of level-1 exists. If a node n_i has recommended a node n_j to be reliable with a certain degree to generate a valid witness and recommendation (Rec_{ij}), a direct trust relation of level-2 exists.Indirect trust is based on the assumption that the trust is somewhat transitive. If a node n_i accepts public key of another node n_j as authentic for which witness has not generated by current node, an indirect trust relation of level-1 exists. Neighbouring nodes are trusted as reliable not by direct issuance of witness and recommendation but it can derive the trustworthiness, in such a way an indirect trust relation of level-2 exists.

Trust Graph Establishment and Malicious Node Exclusion

Integrating recommendations in the key generation process is to increase the reliability about authentication of public keys. The recommendations trust value generated by a trustor node (n_i) for a trustee node (n_j) is denoted as $Tval_{ij}$. When $Tval_{ij}$ is greater, the trustworthiness of n_j will be higher. Trust values are computed by a reputation system based on the collected evidence during interactions among the nodes. After issuance of witness and recommendations to neighbouring nodes, trust graph G is formed

where vertices represent users and edges are defined with three types. A non- weighted solid edge is formed when the node n_i generates only a witness for node n_j without recommending it which means that n_i trusts the n_j's public key. A weighted dashed edge is created when the node n_i has issued only a recommendation without witness for node n_j. The node n_i does not necessarily trusts the public key of n_j. A weighted solid edge is created when a node may be connected to another node by both edges of first type and second type at the same time. In such a case, the superposed edges can be replaced by a single weighted solid edge.

Private-key issuing

This private-key issuing scheme is based on Schnorr's signature and Elliptic Curve Cryptography which was discussed in [5]. This key issuing scheme depends on whether the corresponding node has a root node, single level 1's trustor or multiple level 1's trustor. The root nodes are considered as the initiators of the private-key issuing process. Any node n_i who has no level-1's trustors is considered as a root (i.e $|Trustor_i^1|=0$). Any node who has only one level-1's trustor are considered as single trustor node (i.e $|Trustor_j^1|=1$). Any node having more than one level-1's trustor are considered as multiple trustor node (i.e $|Trustor_j^1|>1$).

Malicious Node Exclusion

An Exclusion Access-control Mechanism [7] based on trust metric evaluation is introduced to detect and isolate the malicious nodes that inject fake trust relations using jury nodes. Whenever the jury node identifies the malicious node, it excludes from the network. There are two different processes update the reputation value.

- In the degradation process, the reputation decreases whenever juror receives an evidence message. The equation for degradation process as follows,

$$`R^i = \max (R^{i-1} - u, 0) \quad (1)$$

- In the improvement process, the reputation value grows periodically to allow nodes to recover the reputation when they perform good actions. The equation for the improvement process as follows,

$$R^i = \min (R^{i-1} + u, R_{max}) \quad (2)$$

Self-Certified Public Key Authentication

Public-keys are self-certified in our trust establishment scheme similar to the approach discussed in Khaled Hamouid et al. [5] Nodes need not to store public-keys or certificates of each other which saves the memory space. Instead of that each node can reconstruct the public keys when they needed. Trust evaluation metric is introduced which allows to evaluate the confidence of the target key through a given trust path.

Evaluating public-key trustworthiness

It is necessary to consider intermediate misbehaving nodes which may cheat authenticity of the target key when public keys are reconstructed based on a given trust path. A trust metric is defined with the set of statements and inference rules. The inference rule and the statements are derived to the confidence of the public-key. By using a probabilistic trust model [5] the inference rules and statements are derived. The node n_3 has multiple trustor nodes such as n_2, n_4 and n_5. Each node generates its witness to the node n_3 which calculate its public key with those witnesses. This public key has high degree of trust worthiness because it is evaluated from the three trustor nodes.

Key Updation

To update any of a node's key, this requires a sequence of key updates of the entire subordinate chain. The key-correction operation causes some problems. If the same node frequently updates their keys, resource consumption will be high. The second problem is that the infinite loop of key correction occurs in a cyclic chain. For the node path n_i -> n_j -> n_l -> n_i, this problem occurs due to the fact that everyone is a trustor of everyone in a cyclic chain. This key updation should be done which is used to avoid the infinite loop key-correction in a cyclic chain. MANETs can dynamically change in size and topology as nodes move,

join and leave the network at any time. Whenever a node leaves the network, it sends a logout request to their trustors and trustees. Whenever a node joins the network, it looks for trustor and trustee nodes.

RESULTS

The simulation was done to analyze the performance of the network for various parameters compared with the UDP [5]. Different metrics are used to evaluate the performance of the network under attacks. The performance analysis was measured with respect to metrics like time delay, computation cost, etc.

Average time delay at malicious environment

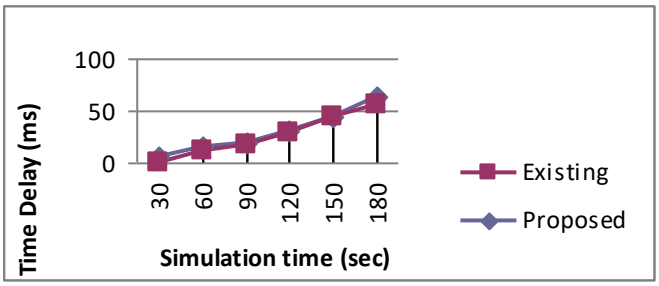

Fig. 3: Average time delay comparison

.....

$$\text{Average time delay} = \frac{\text{(Time at which packets are received} - \text{Time at which packets are sent)}}{\text{Total number of packets received}} \quad (4)$$

Time delay is calculated as in equation 4. [Fig. 3] shows that average time delay with respect to simulation time. Time delay is the time taken for a packet to reach a destination from a source. In the proposed system time delay is somewhat higher than the existing system. Since the proposed system uses trust levels for the authenticated public keys. Hence the proposed system of average time delay is slightly exceeding than existing system.

Computational cost at malicious environment

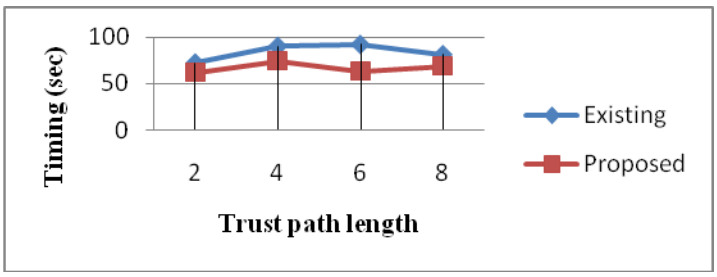

Fig. 4: Computational cost comparison

.....

CONCLUSION

[Fig. 4] shows the computation cost with respect to the simulation time and the trust path length. The existing systems show quite lower than the proposed system. The computation timing will be higher in the existing system because it is using more number of certificates. But the proposed system is certificate-less approach. Our approach requires a single computation of a self-certified key. Hence proposed system has reduced the computational cost even in the larger network.

An enhanced certificate-less trust model for public key authentication in MANETs is designed and also an Exclusion Access-control Mechanism based on trust metric evaluation is introduced to investigate the problem of detecting malicious nodes which may inject fake trust relations. In this work, intermediate misbehaving nodes which may cheat the authenticity were detected and also isolated by improving the trust metrics. The performance and security analysis demonstrate the efficiency of our proposed approach. We have proposed the certificate-less PGP trust model for public key authentication. Detailed analysis has

been done with respect to the parameters. In this work, implementation and performance analysis are presented. Hence, by improving trust metric in MANETs, trustworthy keys are determined through a given trust path. We model the exclusion mechanism and perform a parameter analysis. Simulation results prove that the trust models and an exclusion access control mechanism providing an accurate malicious node detection and exclusion.

CONFLICT OF INTEREST
There is no conflict of interest.

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None

REFERENCES

[1] Huanyu Zhao, Xin Yang and Xiaolin Li, [2013] cTrust: Trust Management in Cyclic Mobile Ad Hoc Networks. IEEE, Vol. 62, No. 6.
[2] [2] Ing-Ray Chen, Jia Guo, Fenye Bao, Jin-Hee Cho. [2014] Trust management in mobile ad hoc networks for bias minimization and application performance maximization. Elsevier, Vol. 19.
[3] [3] Jin-Hee Cho, Ing-Ray Chen, Kevin S. Chan, 2016. Trust threshold based public key management in mobile ad hoc networks', Elseveir, Vol. 44.
[4] [4] Kanimozhi A, Navamani T M, [2016] An Enhanced PGP trust model for public-key authentication in MANET. ICEECE Conference.
[5] Khaled Hamouid, Kamel Adi, [2015] Efficient certificate-less web-of-trust model for public-key authentication in MANET. Computer Communications, Elsevier, Vol. 63.
[6] LeovigildoSánchez-Casado, GabrielMaciá - Fernández, [2015] A model of data forwarding in MANETs for light weight detection of malicious packet dropping. Computer Networks 87.
[7] Lyno Henrique, G Ferraz, Pedro B, Velloso,Otto Carlos M.B. Duarte,[2014] An accurate and precise malicious node exclusion mechanism for ad hoc networks. Elsevier, Vol. 19.
[8] Mohamed M EA, Mahmoud, Xiaodong Lin. [2013] Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks, IEEE.
[9] Mohammad Taqi Soleimani, Mahboubeh Kahvand. [2014] Defending Packet Dropping Attacks Based on Dynamic Trust Model in Wireless Ad Hoc Networks. IEEE Mediterranean Electro technical Conference, Beirut, Lebanon, 13-16.
[10] Saju P John, Philip Samuel, [2015] Self-organized key management with trusted certificate exchange in MANET. Ain Shams Engineering Journal.
[11] Shaheena Khatoon and Balwant Singh Thakur, [2015] Certificate Less Key Management Scheme In Manet Using Threshold Cryptography. IJNSA, 7(2).
[12] Shuaishuai TAN, Xiaoping Li, Qingkuan Dong. [2015] Trust based routing mechanism for securing OSLR-based MANET. Elsevier, 30.
[13] Soumyadev Maity, RC Hansdah. [2014] Self-organized public key management in MANETs with enhanced security and without certificate-chains. Computer Networks 65, ELSEVIER.
[14] Sudha Chinni, Johnson Thomas, Gheorghita Ghinea, Zhengming Shen. [2008] Trust model for certificate revocation in ad hoc networks. Elseveir, Vol. 6.
[15] Zhang Yong, Qian Hai-Feng, [2014] An efficient identity-based secret key management scheme for MANET. Elsevier.
[16] Zheng Yana, Wenxiu Ding, Valtteri Niemi, Athanasios V. Vasilakos. [2014] Two Schemes of Privacy-Preserving Trust Evaluation. Elsevier.