ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse68922020.pdf
https://doi.org/10.30534/ijatcse/2020/68922020

High Security Distributed MANETs using Channel De-noiser and Multi-Mobile-Rate Synthesizer

Murugan G[1], Syed Musthafa.A[2],Mohanraj.B[3],Priyanga.S[4], Krishnan.C[5]

[1]Dept. of Computer Engineering, Vidyalankar Institute of Technology, Wadala East, Mumbai-400037 Maharashtra, India, gopalmurugan0@gmail.com
[2]Dept. of IT, K.S Rangasamy College of Technology, Namakkal, India, syedmusthafait@gmail.com
[3]Dept. of CSE, Mahendra Institute of Technology, Namakkal, India, bmohanrajcse@gmail.com
[4]Dept. of CSE, Mahendra Institute of Technology, Namakkal, India, priyangasadasivam07@gmail.com
[5] Dept. of CSE, Mahendra Institute of Technology, Namakkal, India, ckrishnancse@gmail.com

ABSTRACT

In high security mobile ad-hoc networks (MANETs), user authentication plays an essential role in frustrating unauthorized users on or after retrieving or adjusting the resources of the network. Accordingly, it needs a prevention model and Intrusion detection systems (IDS). Noise channel affected the schedules of time slots for IDS and continuous user authentication. Channel De-Noisier (CDN) introduced to eliminate the malicious adversary with an authenticated user tag of noise status. Mobile Rate Synthesizer (MRS) addressed IDS ineffectiveness in controlling high-speed nodes against intrusion. The NS2 simulator successfully evaluates the CDN-MRS mechanism under varying channel conditions, and noise levels and the outcomes indicate the efficiency of the proposed mechanism in terms of Noise level, Intrusion detection rate, Authentication stratum, and Node energy rate.

Key words: Mobile Rate Synthesizer, Channel De-Noisier, Intrusion Detection, Distributed MANETs, Security.

1. INTRODUCTION

A MANETs (Mobile Ad hoc networks) has a new range of wireless networking, influencing the unrestricted movement of nodes without some necessary infrastructures like switching of mobile nodes or base station. Ad- hoc network, an assembly of nodes interactive with every node by making a multi-hop process. MANET is susceptible to many security attacks because of their structures like open medium, restricted physical safekeeping attacks, change of topology due to dynamic nature, complaisant algorithms used, no centralized checking and organization point, the energy-related mechanism, and lack of the strong defensive line. The security process is a very complex concern in MANET due to its animatedly self-organizing ability is random and due to non-permanent topological network changes that allow the user and the system to work in the way of preexisted infrastructural communication method. Many approaches, such as prevention-based (such as user authentication) and detection-based (detection of intrusion node), helps to safeguard the extraordinary security in MANETs communication. The user authentication might be severe in avoiding the non- accredited users since accessing or changing the resource of the network Manet's security. The authentication of users wants to be continuously achieved and regularly, and then the chances system in an aggressive situation being taken is very high. The authentication of a user (or IDS) might organized in a manner of distribution since both refuge circumstances and resources (e.g., the energy of the node) in the MANETs. They have distributed, continuous authentication of user and detection of intrusion arranging problem expressed in the POMDP multi-armed issue of a bandit. However, in this method, node states at different mobility nodes were not governed, and wireless channel conditions with noises and obstacles not handled. Noise channel affects the schedules of time slots for IDS and continuous user authentication, and hence the execution of authentication and detection of intrusion clue to significant security leak of information.

For the above issues, this paper presents a Channel De-noisier and Multi-Mobile-Rate Synthesizer (CDN-MRS) for continuous authentication of user and IDS for highly sensitive broad MANET distribution. CDN-MRS augmented POMDP

under changeable channel conditions and noise levels on MANET topology. THE proposed CDN-MRS mechanism improves authentication even in noisy situations and detects intrusion at various wireless channel bandwidths.

2. LITERATURE REVIEW AND RELATED WORK

An intrusion detection mechanism used to examine and handle a flow of enormous network performance by minimizing the module computation time. In a real-time application, it initially establishes a prototype of detecting intrusion mechanism tests, in addition to analysis, and investigates the associated data. In abstract design, it makes different algorithms that based on heuristic computation, and after that applies in module investigation and judgment in intrusion detection approach [1].

MANET does not have a centralized way of networking such a way that the mobility of nodes modifies its position several times. Because of that environment, the network provides a variety of category attacks (active and passive) are potential which influence the performance of the network [2]. Different Attacks are found utilizing the K-Means algorithm and choose the appropriate listing of nodes through the head cluster. Maintenance of topology is performed and for detecting attacks continuously. IDS tools have been analyzed, prepared for comparison by different systems through their attributes and properties [3]. The flooding attacks measured as one of the types of DoS attacks to use the resource of the networks. This attack affects the performance of the network by various metrics. Preventive action and detection mechanism of a type of nodes should be avoided, which gives better performance of the network. AIF_AODV has two algorithms to ignore the damages of the Flooding attack and to isolate the network from the attacker node[4]. The routing protocols are essential in MANETs that provide the security aspects among the nodes; thus, the exchange of information carried out by the hiding node identity, and the routes are as of outside the observers[6]. The co-operation based bait mechanism is introduced to detect the evil nodes which destroy the network in MANET[8]. The authors in [11] projected a useful approach to merging the authentication and detection of intrusion.

On the other hand, the scheme in [12] is a centralized scheme, by which the entire network gets formulated in a single partially based the observable Markov decision process (POMDP). The method of the POMDP would be more complexly determined, while the POMDP develops exponentially with the help of many biometric-based sensors and IDSs [13]. Because of the above-said reason, an innovative scheme should be prepared for MANET with an enormous amount of spread nodes.

3. CHANNEL DE-NOISIER AND MULTI-MOBILE-RATE SYNTHESIZER FOR HIGH SECURITY DISTRIBUTED MANETs

In this section, the proposed system develops an efficient combinatorial mechanism for continuous user authentication and IDS in highly sensitive broad MANET distribution. The proposed mechanism is named as Channel De-noisier, and Multi-Mobile-Rate Synthesizer (CDN-MRS) augment POMDP under varying channel conditions and noise levels on MANET topology. Channel De-Noisier (CDN) is introduced to eliminate the malicious adversary with an authenticated user tag of noise status [14]. CDN measured statistical noise levels for the varied topology of highly hostile MANET environments. The noise indicator is arrived with training samples based on a multi-simulated wireless network and identifies the malicious activity and the actual noise in the network. Mobile Rate Synthesizer (MRS) addressed IDS ineffectiveness in controlling high-speed nodes against intrusion. MRS governs the node speed and classifies into three variants, i.e., standard, high, and very steep. In the case of reasonable default, POMDP quickly detects IDS, whereas, in the case of high and very high mobile nodes, POMDP can not detect [15] [16]. High and very high mobile nodes are monitored more accurately by MRS at different positions in the network topology. Position observers identify the intrusive nature of the mobile node. In noisy conditions and detect intrusion at various wireless channel bandwidths. Therefore, CDN-MRS increases the detection rate of POMDP and also minimizes the fake reception and fake Rejection rates compared to existing POMDP. THE proposed CDN-MRS mechanism improves authentication. Even Figure 1 demonstrates the Channel De-noisier and Multi Mobile-Rate Synthesizer for High-Security Distributed MANETs, which helps to understand the different ranges of node distribution authentication strategy and the noise variance detection [17].

3.1 DISTRIBUTED MANETs

Imagine that the MANET has a constant system of authentication and IDSs, for detecting intrusions. In MANET, mobile nodes have limited battery life, limited memory, processing capability, and relay data (act as routers). Mobile nodes distributed across the region and MANET [18] environment has no centralized authority which deployed in an adverse or hostile environment.

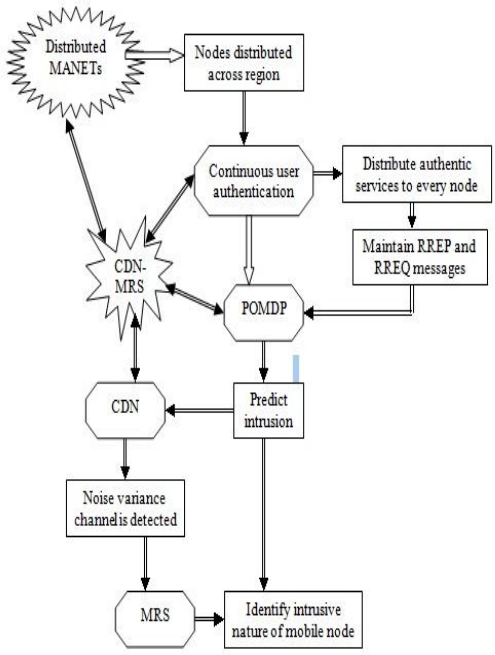

Figure 1: Channel De-Noisier and Multi-Mobile-Rate Synthesizer for High-Security Distributed Manets

The mobile network is divided into different distributed regions in which each area is formed with a similar number of nodes. Each group has a unique group ID and obtained a hierarchical organization [19] [20]. There is a limited direct monitor capability to the Neighboring nodes. Therefore, the way of monitoring the work can be allowed to proceed further. The method performs two different operations: intrusion detection and user authentication. IDSs can function at every time instant to observe the system. Authentication might be executed each time instantaneously as well. Though, authentication and intrusion detection might be consuming a considerable quantity of energy, which turns to unease for energy- controlled devices in MANET.

3.1 CONTINUOUS USER AUTHENTICATION

Continuous user authentication distributes the authentic services to every node. Beacon packets and beacon nodes are used in this process. Deployment knowledge confirms beacon integrity, which detects run time violations. Behaviors of routing protocol are specified, and distributed trust management is deployed. In Continuous User Authentication, users act as certifying authority. Here, many nodes can sign another's public key by its private key to set up the network of trust without the need for any trust root authentication. Rely only lying on the groups and faith by authenticated introducers. RREP and RREQ [21] [22] messages are maintained to identify and respond to routing misbehaviors. Every node verifies that his data was forwarded correctly. Routes have been rated, and then more reliable ones are used.

3.2 IDS with Partially Observed Markov Decision Process (POMDP)

In this section, IDS with POMDP (Partially Observed Markov Decision Process) [24] [25] is discussed. The utilization of Markov Chains characterizes the normal behaviors of users. In each region in distributed MANET, alerts can be generated locally inside the zone. Gateway nodes broadcast signals within the region based on the observed Markov decision process. The message exchange format has facilitated the interoperability of IDS agents. Markov Decision process makes cross-feature analysis to identify intrusive node behaviors and capture correlation patterns. These cross-feature analyses are characterized based on topology and route activities. POMDP has been Identified temporal correlation between one feature and all other features. It predicts intrusion in normal circumstances and also improbable attack scenarios.

3.3 Channel De-Noisier and Mobile-Rate Synthesizer (CDN-MRS)

In Channel De-noisier and Mobile-Rate Synthesizer (CD-MRS), the receiver and the transmitter are coordinated correctly into which a single channel might transmit the data. The signal appears towards inarticulate interval impulse noise in favor of eavesdroppers. Because the messages spread across several frequencies, the interference will be reduced. Noise agent associated with each node performs ID and response individually. Construct & select feature set are depends upon the Noise level, distance, velocity, and the number of hops. CDN detects noise variance in the channel. Channel De-Noisier (CDN) eliminate malicious adversary with authenticated user tag of noise status. Trust model with chain de-noisier authentication maintains the trust values of different nodes. Integration of Mobility and ID in MANET utilize link change rate as an indication of mobility. Collaborate-channel de-noisier and rate synthesizer used to detect abnormal events and false alarm with surrounding nodes to confirm. Mobile Rate Synthesizer (MRS) addressed IDS ineffectiveness and Controlled the high-speed nodes against intrusion. MRS reduced node speed as three types, named, healthy, high, and very high. POMDP governs normal speed nodes against intrusion attacks. High and very high mobile nodes are monitored accurately at different positions in varying topology by CDN-MRS. Position observers identify the intrusive nature of the mobile node. The proposed mechanism, CDN-MRS, is projected to present continuous user authentication and IDS intended for a manet application under varying channel conditions noise levels on MANET topology [23].

4. Simulation Discussions and Results on CDN-MRS

In this part, the NS2 simulations are used toward the comparison of the proposed CDN-MRS performance and existing scheme POMDP, and also the performance of the other two methods. Considering the simulation circumstances, a graph is exposed in figure 2. It is generated through the measurements of Intrusion detection given in the following table 1.

Table 1: Intrusion detection rate (%)

Noise level (%)	Intrusion detection rate (%)	
	CDN-MRS	POMDP
1	92.23	78.25
2	91.26	76.54
3	91.05	76.27
4	89.54	69.2
5	89.03	67.58

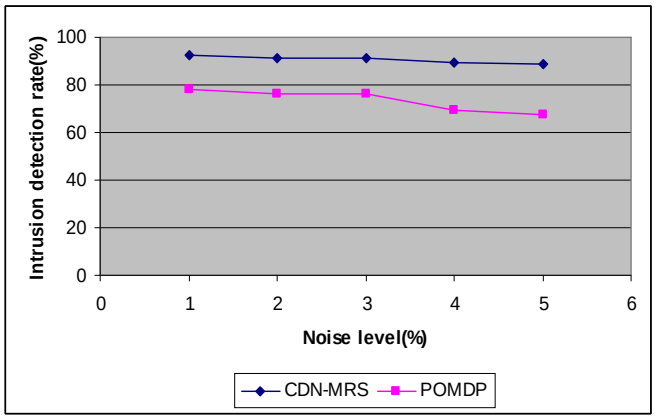

Figure 2: Intrusion detection rate (%)

From the above graph, CDN-MRS achieves relatively high performance than the existing system, POMDP, in terms of high intrusion detection rate. THE current POMDP method is having less intrusion detection rate, CDN-MRS high. When there is a low-level noise presented, both ways display a high detection rate. When the noise level gets increased, the detection rate decreases accordingly. Figure 2 shows a better performance of CDN-MRS in terms of the high intrusion detection rate than the existing method. CDN-MRS achieves a 14% to 22% upper intrusion detection rate when compared with POMDP.

The below graph in figure 3 produced through the measurement authentication specified in table 2.

Table 2: Authentication (%)

Mobility(m/s)	Authentication (%)	
	CDN-MRS	POMDP
2	94.43	89.81
4	94.33	82.18
6	94.02	84.34
8	91.17	76.13
10	91.23	72.21

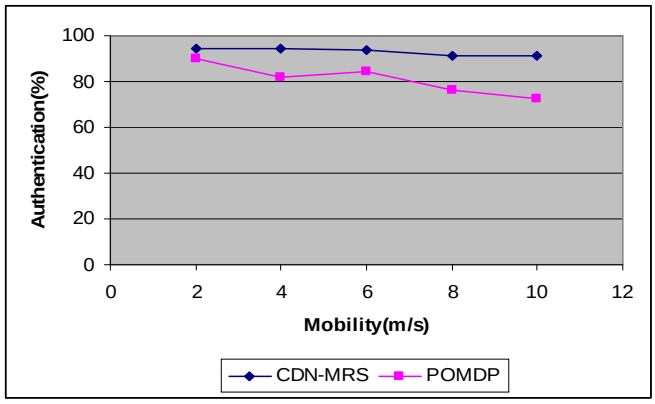

Figure 3: Authentication (%)

Figure 3 presents the comparison result of the Authentication stratum of Proposed CDN-MRS and existing POMDP. CDN-MRS attains the best performance possible on this metric because it used Channel De-Noisier (CDN) to eliminate the malicious adversary with an authenticated user tag of noise status. An existing method, POMDP, has a moderate authentication stratum. All the curves show a more or less yet steady descendant when mobility increases. Figure 3 shows a better Authentication stratum of CDN-MRS that shows a 5% to 19% higher Authentication stratum than POMDP.

Table 3: Energy consumption (%)

Node density	Energy consumption (%)	
	CDN-MRS	POMDP
10	1.46	2.33
20	1.49	2.57
30	1.53	2.78
40	1.74	3.12
50	1.77	3.34

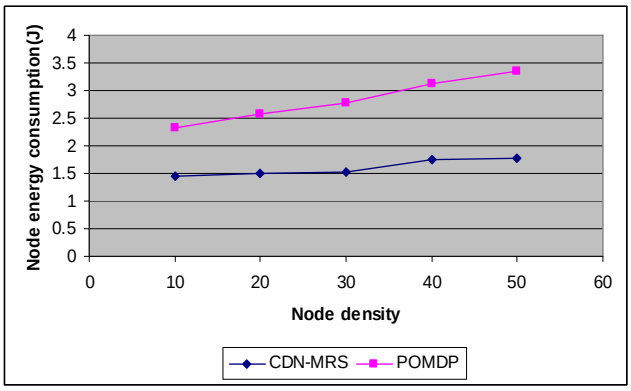

Figure 4: Energy consumption (%)

The simulations additionally use many numbers of nodes in the direction of authenticating the performance of the proposed approach in terms of energy consumption. Figure 4 presents the assessment result of consumption Energy in the Proposed CDN-MRS and existing POMDP. CDN-MRS consumes less energy, whereas POMDP consumes more energy. Figure 4 shows the best performance of CDN-MRS, which shows 17% to 34% less energy consumption than POMDP [26].

4. CONCLUSION

In this paper, a combinatorial mechanism for continuous user authentication and IDS is proposed in a highly sensitive large distributed MANET. This mechanism is developed based on the Channel De-noisier approach (CDN), and Multi Mobile-Rate Synthesizer approach (MRS) to high-security MANETs distributed augment PODMP under different channel conditions and varying noise levels on MANET environments. Channel De-Noisier (CDN) has been used to remove the malicious adversary with an authenticated user tag of noise status. Mobile Rate Synthesizer (MRS) utilized to IDS ineffectiveness in controlling high-speed nodes against intrusion. Proposed CDN-MRS increased authentication level even in noisy conditions and enlarged Detections of intrusion level at different wireless channel bandwidths. Performance results illustrate that proposed CDN-MRS exhibits 14% to 22% high intrusion detection rate, 5% to 19% more upper Authentication stratum, and 17% to 34% less energy consumption than the existing POMDP scheme.

REFERENCES

1. Zakki Ul Rehman Khan and Ms.Ankita Sharma. **Security Aspects of MANETs: A Review**, *International Journal of Computer Science and Mobile Computing*, vol. 8. Issue. 7, pp. 40–44, 2019.
2. H. Fathima and Dr. A.Syed Musthafa. **Intrusion Detection System Based on Ant Colony System**, *Global Journal of Computer Science and Technology: H Information & Technology*, vol. 1, no. 4, 2017.
3. K.Bala and A.Chandra Sekar. **An Efficient Multi-Level Intrusion Detection System for Mobile Ad-Hoc Network Using Clustering Technique**, *International Journal of Engineering and Advanced Technology*, vol 8, Issue 6, pp 1977-1985, 2019. https://doi.org/10.35940/ijeat.F8291.088619
4. Prosanta Gope. **Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol**, *security, and communication reviews*, vol. 2019. https://doi.org/10.1155/2019/8249108
5. Dr. Gorine and Rabia Saleh. **Performance Analysis of Routing Protocols in Manet Under Malicious Attacks**, *International Journal of Network Security & Its Applications*, vol. 11, no.2, 2019. https://doi.org/10.2139/ssrn.3368178
6. Swetha M. S and Thungamani M. **A Novel Approach to Secure Mysterious Location-Based Routing For Manet**, *International Journal of Innovative Technology and Exploring Engineering*, vol. 8 Issue 7, 2019.
7. Hu J., Yu X., Qiu D., and Chen H., Jan. **A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection**, *IEEE Network*, vol. 23, pp. 42–47, 2009. https://doi.org/10.1109/MNET.2009.4804323
8. A.Syed Musthafa**. Co-operative bait detection against malicious nodes attacks in MANET**, *International Journal on Concurrent Applied Research in Engineering and Management*, vol. 4, 2016.
9. Waleed Alnumay and Uttam Ghosh. **A Trust-Based Predictive Model for Mobile Ad Hoc Network**, *Internet of Things sensors (Basel)*, vol 19(6), 2019. https://doi.org/10.3390/s19061467
10. Krishnamurthy. V and Wahlberg. B. **Partially observed Markov decision process multiarmed bandits—structural results**, *Math. of Oper. Res.*, vol. 34, pp. 287–302, May 2009.
11. Mohammad Riyaz Belgaum and Shahrulniza Musa. **Secured Approach towards Reactive Routing Protocols Using Triple Factorin Mobile Ad Hoc Networks**, *Journal of Emerging Technologies in Computing*, vol. 3, no. 2, 2019. https://doi.org/10.33166/AETiC.2019.02.004
12. S.Sudhakar, V.Vijayakumar, C.SathiyaKumar, V.Priya, LogeshRavi, V.Subramaniyaswamy, **Unmanned Aerial Vehicle (UAV) based Forest Fire Detection and monitoring for reducing false alarms in forest-fires**, *Elsevier- Computer Communications* 149 (2020) 1–16, https://doi.org/10.1016/j.comcom.2019.10.007
13. Shengrong Bu, Fei Richard Yu Peter Xiaoping Liu, and Helen Tang. **Structural Results for Combined Continuous User Authentication and Intrusion Detection in High-Security Mobile Ad-Hoc Networks**, *IEEE Transactions on Wireless Communications*, DOI:10.1109/TWC.2011.071411.102123 2011.

14. R.Vasanthi, R.Jayavadivel, K.Prasadh, J.Vellingiri, G. Akilarasu, S.Sudhakar, P.M.Balasubramaniam, **A novel user interaction middleware component system for ubiquitous soft computing environment by using the fuzzy agent computing system**, *Journal of Ambient Intelligence and Humanized Computing* (2020), Springer, doi.org/10.1007/s12652-020-01893-4.
15. Jagadeesh Gopal, Vellingiri J, Gitanjali J, Arivuselvan K, Sudhakar S, **An Improved Trusted On-Demand Multicast Routing with QoS for Wireless Networks**, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.9, No.1, Feb. 2020,pp:261-265,https://doi.org/10.30534/ijatcse/2020/39912020.
16. Satheesh N, Sudha D, Suganthi D, Sudhakar S, Dhanaraj S, Sriram VP, Priya V, "**Certain improvements to Location aided packet marking and DDoS attacks in internet**," *Journal of Engineering Science and Technology*, Vol. 15, No. 1 (2020), pp: 94 - 107, School of Engineering, Taylor's University.
17. Sathiya Kumar C, Priya V, Sriram V P, Sankar Ganesh K, Murugan G, Devi Mani, Sudhakar S, "**An Efficient Algorithm for Quantum Key distribution with Secure Communication**, *Journal of Engineering Science and Technology*, Vol. 15, No. 1 (2020), pp:77-93, School of Engineering, Taylor's University.
18. S.Sudhakar, N.Satheesh, S.Balu, Amireddy Srinish Reddy, G.Murugan, 2019, "**Optimizing Joins in a Map-Reduce for Data Storage and Retrieval Performance Analysis of Query Processing in HDFS for Big Data,"** *International Journal of Advanced Trends in Computer Science and Engineering, (IJATCSE)*, Vol.8, No.5, pp:2062-2067, DOI:10.30534/ijatcse/2019/33852019.
19. Sudhakar Sengan & Chenthur Pandian S, 2016, '**Hybrid Cluster-based Geographical Routing Protocol to Mitigate Malicious Nodes in Mobile Ad Hoc Network**, *International Journal of Ad Hoc and Ubiquitous Computing*, ISSN online: 1743-8233; ISSN print: 1743-8225, Vol.21, No.4, pp:224-236. https://doi.org/10.1504/IJAHUC.2016.076358
20. Sudhakar Sengan, Chenthur Pandian S, 2015, "**Analysis of attribute aided data aggregation through dynamic routing in wireless sensor networks**," *Journal of Engineering Science and Technology, School of Engineerin*g, Taylor's University, Vol. 10, No.11 (2015) 1465-1476ISSN:1823-4690.
21. A.U. Priyadarshni, Dr.S.Sudhakar, 2015," **Cluster Based Certificate Revocation by Cluster Head in Mobile Ad-Hoc Network**," *International Journal of Applied Engineering Research*, ISSN 0973-4562 Vol. 10 No.20, pp:16014-16018.
22. Sudhakar Sengan & Chenthur Pandian S, 2013,'**Trustworthy Position-Based Routing to Mitigate against the Malicious Attacks to Signifies Secured Data Packet using Geographic Routing Protocol in MANET**', *WSEAS Transactions on Communications*, vol.12, no.11, pp. 584-2013.
23. Sudhakar Sengan & Chenthur Pandian S, 2013, '**A Trust and Co-Operative Nodes with Affects of Malicious Attacks and Measure the Performance Degradation on Geographic Aided Routing in Mobile Ad Hoc Network**,' *Life Science Journal*, Vol. 10, No. 4s, pp. 158-163, 2013.
24. Sudhakar Sengan & Chenthur Pandian S, 2012, '**An Efficient Agent-Based Intrusion Detection System for Detecting Malicious Nodes in MANET Routing**,' *International Review on Computers and Software (I.RE.CO.S.),* Vol. 7, No. 6, pp. 3037-304.
25. Sudhakar Sengan & Chenthur Pandian S, 2012, '**Secure Packet Encryption and Key Exchange System in Mobile Ad hoc Network**,' *Journal of Computer Science*, No. 6, pp. 908-912. https://doi.org/10.3844/jcssp.2012.908.912
26. Sudhakar Sengan & Chenthur Pandian S, 2012. '**Authorized Node Detection and Accuracy in Position-Based Information for MANET,'** *European Journal of Scientific Research*, Vol. 70, No. 2, pp. 253-265.