Asian Journal of Scientific Research

ISSN 1992-1454

OPEN ACCESS Asian Journal of Scientific Research

ISSN 1992-1454
DOI: 10.3923/ajsr.2019.369.375

Research Article
Defending against Medium Access Control and Network Layer Misbehavior Attacks by Monitoring Nodes in MANET

[1]Abhishek Ranjan, [2]Venu Madhav Kuthadi, [3]Tshilidzi Marwala and [4]Rajalakshmi Selvaraj

[1]Faculty of Engineering and Built Environment, University of Johannesburg, South Africa
[2]Department of AIS, University of Johannesburg, South Africa
[3]Faculty of Engineering and Built Environment, University of Johannesburg, South Africa
[4]Department of Computing BIUST, Botswana

Abstract
Background and Objective: In Mobile *Ad Hoc* Network (MANET) existing misbehavior detection systems rarely consider both MAC and network layer misbehaviors. Hence the main objective of this work was to develop misbehavior detection and defense techniques for both MAC layer and network layer attacks. **Materials and Methods:** This paper proposed a cross-layer based misbehavior detection and defense technique (CLMDD) for MANET. Ant Colony Optimization (ACO) technique was applied to select reliable monitoring nodes which detected the misbehaving nodes. Then in receiver detection module, back off cheating was analyzed. In audit module, greedy nodes were detected which performs the Media Access Control (MAC) layer misbehaviors. **Results:** The proposed CLMDD technique was simulated in NS2 and compared with the Audit-based Misbehaviour Detection (AMD) technique. By simulation results, it had been shown that CLMDD attained reduced packet drop, energy consumption and normalized overhead when compared to AMD technique. **Conclusion:** It can be concluded that CLMDD had been considered as the best approach for detecting and defending the misbehavior attacks in MANET.

Key words: Mobile *ad hoc* network, intrusion detection, misbehavior detection, cross-layer based, ant colony optimization

Received: October 24, 2018 Accepted: November 28, 2018 Published: June 15, 2019

Citation: Abhishek Ranjan, Venu Madhav Kuthadi, Tshilidzi Marwala and Rajalakshmi Selvaraj, 2019. Defending against medium access control and network layer misbehavior attacks by monitoring nodes in MANET. Asian J. Sci. Res., 12: 369-375.

Corresponding Author: Abhishek Ranjan, Faculty of Engineering and Built Environment, University of Johannesburg, South Africa Tel: +266 51651682

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

MANET consists of frequently moving nodes which self organize themselves and has no fixed network infrastructure. Each node in MANET operates as a device and a router which can forward the data to its neighbors. MANETs are mainly employed in military applications, video conferencing, emergency and rescue operations etc. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery[1,2]. The main issues of MANET are limited capacity, energy constrained devices and sharing of limited bandwidth[3,4].

In MANETs, security has been identified as one of the major challenges. Some of the attacks targeted at MANET are black hole, worm hole, Denial of Service (DoS), Sybil etc[5]. In misbehavior attacks, the nodes may be compromised and important data packets may be dropped without forwarding to others[6,7]. Intrusion detection and prevention provides a way to protect MANETs from attacks by external or internal intruders.[8,9]. Existing solutions for misbehavior detections mostly involve monitoring the behaviors of nodes or providing some rewards to the well behaving nodes. Since the process of monitoring of nodes should be repeated across multiple hops along a route, it incurs huge communication overhead. Moreover, intermediate monitoring nodes fail to detect the selective dropping attack[10]. Some of the examples of misbehaving detecting methods are credit-based systems and reputation based systems[11].

Existing misbehavior detection systems rarely consider both MAC and network layer misbehaviors. In real-time detection of MAC layer misbehavior[12], throughput and inter-packet interval time are considered to detect the attackers. However, this technique does not detect the backoff cheating technique. Cross-layer based stealthy attack detection technique (SAMRP) has been proposed[13] to detect and isolate the MAC layer attacks. But it has to analyze large volumes of traffic logs collected from the network. So it has resulted in high time complexity and cost.

In HsF-MAC[14] scheme, the back off value is recalculated and checked by the receiver to detect the backoff cheating technique. But it does not detect the greedy nodes which perform other type of MAC layer misbehaviors. The anomaly based heavyweight module[15] did not consider MAC layer attacks.

A sybil attack detection scheme[16] based on signed response (SRES) authentication mechanism has been proposed. A cross-layer based distributed and cooperative IDS with Dempster-Shafer evidence theory (CID) system[17] has been developed. The system includes a local detection which continuously monitors the network activity. When the local detection engine detects malicious activity, it turns on IDS in a node. The misuse detection with the anomaly detection systems were combined[18] to save the cost associated with resource constraints and security requirements. Fuzzy based IDS[19] has been developed to detect the malicious behavior of nodes and to identify the type of attacks. A lightweight, scalable and distributed detection approach[20] has been designed which is based on the difference in movement patterns of Sybil nodes and legitimate nodes. An improved detection mechanism[21] has been developed for detecting the physical jamming attacks in MANET.

Hence, the main objective of this research trial was to develop a misbehavior detection scheme for detecting both MAC layer and network layer misbehaviors.

In this study, a cross-layer based misbehavior detection and defense technique for MANET is proposed.

MATERIALS AND METHODS

Overview: In this paper a cross-layer based misbehavior detection and defense technique for MANET was proposed where ACO technique is applied to select trusted monitoring nodes that can easily identify any misbehavior attack. Then in receiver detection module, backoff cheating is analyzed. In audit module, greedy nodes are detected which performs the MAC layer misbehaviors.

This technique involves three phases:

- Selection of monitoring nodes
- Receiver detection module
- Auditing module

Selection of monitoring nodes: This section describes about the selection of monitoring node by applying ACO technique. Due to above mentioned unique feature of ants, ACO technique was applied to get optimized monitoring node. Based on the concentration of pheromone deposit in form of next hop information, the monitoring node has been selected.

For a node η to become monitoring node, following condition need to be satisfied:

- Neighbor of M_2
- Neighbor of previous hop from M_2, assume as M_1

Then, η is called as monitoring node over the link $M_1 \rightarrow M_2$.

Table 1: Observation table

Routing information updated by F-ANT and B-ANT during its trial		
Duplication of packet (C_1)	Hash of payload (C_2)	Dropped or delayed (check the time limit) (C_3)

Let $G(M_1, M_2)$ be a set of participating monitoring nodes. The ant agent has checked the following condition to update the information about the visiting hop in the routing table:

- C_1: Packet the hop contain must not be fabricated or duplicated
- C_1: It should not be corrupted (matching hash of payload)
- C_1: Packet should be delivered within time limit τ

The ants has updated this information in the routing table and the hop which meets all these conditions was considered as the monitoring node as shown in Table 1.

In ACO technique, ant spreads randomly all over the network to collect the next hop information. This can be explained as below in Algorithm 1:

Algorithm 1

Let S and D be the source and destination nodes
Let MN be the monitoring node:

- Pheromone was set to zero
- FA was generated by S with a threshold value PH_τ in order to send data to D
- MN was considered based on the next hop information which is decided based on the value of pheromone deposit, i.e., the hop which satisfies all the above mentioned conditions i.e., C_1, C_2 and C_3:

$$PH_V = H(C_1 \cap C_2 \cap C_3) \rightarrow \eta \tag{1}$$

- FA moved through M_i by using the rule described in step 3
- Pheromone PH_V was compared with the considered threshold PH_τ

If $PH_V > PH_\tau$:
Then, FA stayed on the same path and updated routing table till it reach D
Else if $PH_V < PH_\tau$:
Then, FA discarded the path and did not update the routing table.
End if:

- Once FA reaches D, it delivers all the gathered information to BA
- BA then followed the same path but in opposite direction and keeps on updating the routing tables with new information[22]
- Once BA reaches S, then it transmits all the information to S
- Based on this information, S has selected the monitoring node

Table 2 represents the frequent updates by ants to find the best monitoring nodes.

The proposed technique helps to find the best monitoring node based on the concentration of pheromone. In this way the ant spreads over the network and collects the previous and the next hop information and updates this information in the routing table[23]. Based on this monitoring node is selected to detect any kind of misrouting packet drop attack. For this an observation table is made based on report about the next hop information in the routing table.

Receiver detection module: Receiver detection module is presented in Algorithm 2.

Algorithm 2

W checks the modified back off value using hash function [X] to check the deviation:

$$X = h\ (fct\ (y, a))\bmod 2^{\alpha-1}\ z_{min} \tag{2}$$

Where:

$$fct\ (y, a) = (y \oplus \alpha)$$

If W finds any significant deviation for any node N_i,
Then:

- C→True
- S→CHEAT
- Records R and V

If (R<LT) and (V>UT)
Then:

- MAC layer misbehavior attack is detected.
- C→True
- S→GREEDY
- $R \xrightarrow{\text{MISSALARM}} M_i$
- M_i verifies node ID and its S

If S = CHEAT
Then:

$$M_i \xrightarrow{\text{*Cheating node details}} N_i$$

Else if S = GREEDY
Then:

- Auditing is performed

End if
End if
End if
End if

In this algorithm, the modified back off value has been checked by the receiver using hash function (Eq. 2) for any deviation. If it finds any significant deviation, suspected flag was set for that node and attack type was changed as CHEAT. If throughput T is below LT and the inter-packet interval (IPI)

Table 2: Pheromone deposit

Pheromone item		Index	Significance	Notation
Attempt success	PH_S	1	Monitoring node	Represents best monitoring node
Attempt failure	F_PH_S	2	Monitoring node	Represents conditions are not satisfied

Table 3: Simulation settings

Number of nodes	100
Size of the topology	1000×1000 m
MAC protocol	IEEE 802.11
Traffic model	CBR
Propagation model	Two ray ground
Antenna model	Omni antenna
Initial energy	10.0 joules
Transmitting power	0.8 watts
Receiving power	0.5 watts

time is above UT, then a MAC layer misbehavior attack was detected. Then the suspected flag was set and attack type was changed as GREEDY. The receiver then sends a misbehavior warning message to all the monitoring nodes which contains the details of suspected node and its attack type. If the attack type is CHEAT, then the details of cheating node was broadcast to other nodes so that further requests from that node can be rejected. On the other hand, if the attack type is GREEDY, auditing module is triggered.

Audit module: If the attack type is GREEDY, the audit module was invoked. In this module M_i requests an AUDIT CLAIM request to N_{i-1}, N_i and N_{i+1}. The requested nodes send the reply to the monitoring nodes which consists of number of packets received and forwarded by them. By cross-checking the reply with other monitoring nodes, the exact location of misbehaving node can be tracked. The details identified misbehaving node is then broadcast to all other nodes so that any further communications to that node can be blocked.

This process is illustrated in Algorithm 3:

Algorithm 3

Note: Packets in P are compactly represented by using Bloom filter in an ρ-bit vector λ_i with $\rho<<|P|$.

- M_i selects T_{au} and S_{au} and forwards AUDIT_CLAIM_REQ message through N_{i-1}, N_i and N_{i+1}
- If AUDIT_CLAIM_REQ message is dropped, then M_i choose $P = \phi$ and hence $au_i = 0$
- When N_{i-1}, N_i and N_{i+1} is audited, a Bloom filter (AUDIT_CLAIM_REP) was constructed for P that it had received and forwarded, starting from any received $S\geq S_{au}$ until $T_{au}+S_{au}$
- For $P = \phi$, initially, all ρ-bits of λ_i were set to zero
- $p\epsilon P$ is included as a member in bloom filter through X_j, where X_j ranges in $\{1,\cdots, \rho\}$
- The relevant bits X_j (p) of vector λ_i were set to 1
- To verify whether $x\epsilon X$ occurs in P, x has hashed e times using X_j and the corresponding bits were verified against the vector λ_i
- If a zero is found in the related location in λ_i

  Then:
    $x\notin P$
  Else:
    $x\epsilon P$ occurs with high probability
  End if:

- After including all packets received between S_{au} and $S_{au}+T_{au}$ in λ_i, M_i signs λ_i and sends through the reverse path
- During authentication

  If the signature check of λ_i fails
  Then:
    M_i discards it
  Else
    It computes σ
  End if

Here:

$$\sigma = \frac{\sum_{i=1}^{n} \mu_i |P_i|}{\sum_{i=1}^{n} \mu_i |Q_i|} \tag{3}$$

where, μ_i represents weight, $i = 1,\cdots n$.
P and Q represents the set of data packets
For eliminate storage overhead, M_i performs the following:

- For each data packet, creates its own Bloom filters τ_j
- Computes $|P_j|$, $\forall j$:

$$\left|P_j\right| = |Q_j \cap P| \approx \left|Q_j\right| + \left|P\right| - \frac{\log\left(\frac{<\lambda_i,\tau_j>}{\Omega}\right) + (1-\frac{1}{\Omega})^{e|Q_j|} + (1-\frac{1}{\Omega})^{e|P|}}{e\log(1-\frac{1}{\Omega})} \tag{4}$$

Evaluates the audit claim:

$$AC_i = \begin{cases} 1, & \sigma \geq \psi_0 \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

where, ψ_0 indicates the threshold value below which an audit claim is subjected to significant packet loss:

- If $\sigma<\psi_0$, then M_i claims that packets were not forwarded to the next hop
- The details identified misbehaving node is then broadcast to all other nodes so that any further communications to that node can be blocked

Experimental design: The proposed cross-layer based Misbehavior Detection and Defense Technique (CLMDD) has been simulated in NS2 and compared with the Audit-based Misbehavior Detection (AMD)[10] technique. The performance of these two techniques is evaluated in terms of the metrics end-to-end delay, packet delivery ratio, average residual energy and normalized control overhead. The simulation settings are shown in Table 3.

RESULTS AND DISCUSSION

In this experiment, the number of attackers launching packet dropping attacks is varied from 5-25.

The end-to-end delay of both the techniques is depicted in Fig. 1. When the attackers are increased, the delay of AMD increases from 6.3-7.9 sec and the delay of CLMDD increases from 4.8-5.8 sec. The packet delivery ratio of both the techniques is shown in Fig. 2. As shown in the Fig. 2, the packet delivery ratio of AMD decreases from 0.44-0.24 and the packet delivery ratio of CLMDD decreases from 0.57-0.35. The average packet drop measured for both the techniques is shown in Fig. 3. As seen in the Fig. 3, packet drop of AMD increases from 8033-21859 and the packet drop of CLMDD increases from 3530-8319. The average residual energy measured for both the techniques is shown in Fig. 4. As seen from the Fig. 4, the residual energy of AMD decreases from 6.9-6.1 joules and the residual energy of CLMDD decreases from 7.39-6.89 joules. The normalized control overhead occurred for both the techniques is shown in Fig. 5. When the attackers are increased, the normalized overhead of AMD increases from 0.5464-0.7304 whereas the normalized overhead of CLMDD increases from 0.2164-0.3978.

As shown in Table 4, CLMDD achieves performance improvement in terms of all the metrics, when compared to AMD.

When the number of misbehaving nodes is increased, it leads to more packet drops, resulting in degradation of delivery ratio and residual energy of nodes. Moreover, it results in increased overhead also due to the messages exchanged during detection phase. However, since CLMMD handles misbehavior attacks at MAC layer and intermediate packet drops, the packet delivery ratio of CLMDD was significantly high. Since less number of monitoring nodes is needed in CLMDD, the average residual energy of nodes became high and normalized overhead became less.

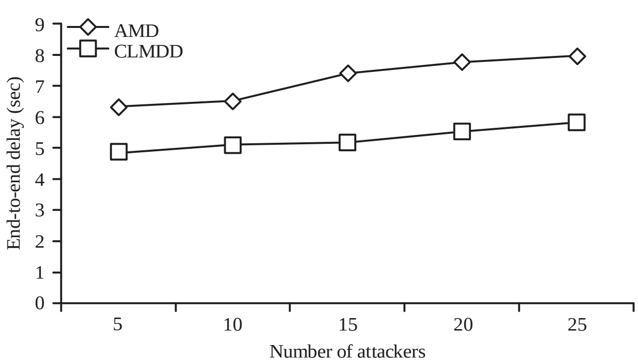

Fig. 1: Delay measured for cross-layer based misbehavior detection and defense technique

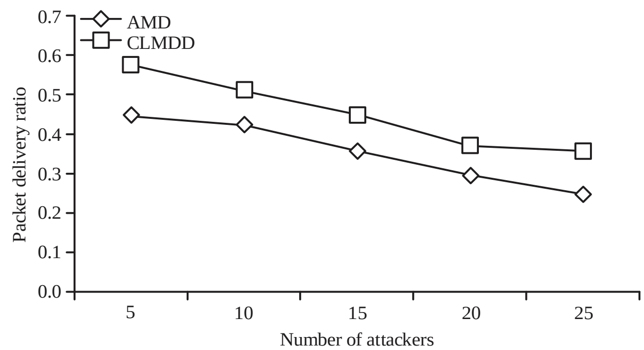

Fig. 2: Packet delivery ratio for cross-layer based misbehavior detection and defense technique and audit-based misbehavior detection algorithms

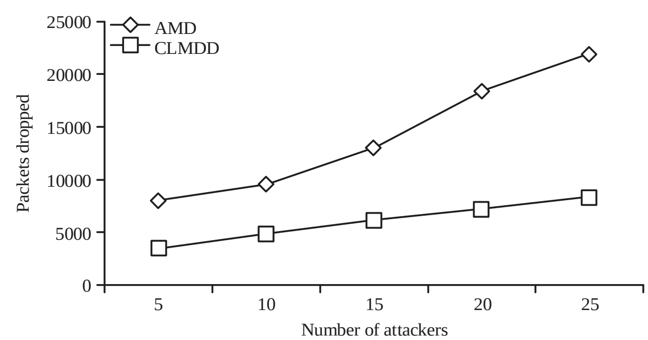

Fig. 3: Packet drop for cross-layer based misbehavior detection and defense technique and audit-based misbehavior detection algorithms

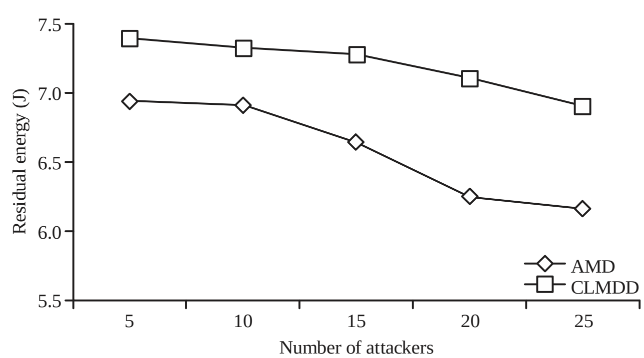

Fig. 4: Residual energy for cross-layer based misbehavior detection and defense technique and audit-based misbehavior detection algorithms

Table 4: Percentage wise improvement of CLMDD over AMD

Number of misbehaving nodes	Improvement in residual energy (%)	Reduction in delay (%)	Improvement in delivery ratio (%)	Reduction in normalized overhead (%)	Reduction in packet loss (%)
5	6.1	22.4	21.6	60.3	56.0
10	5.6	21.8	17.2	62.5	48.9
15	8.6	30.1	20.7	60.4	52.5
20	11.9	28.7	20.1	46.7	60.6
25	10.7	26.8	30.4	45.5	61.9
Average	8.6	26.0	22.0	55.0	56.0

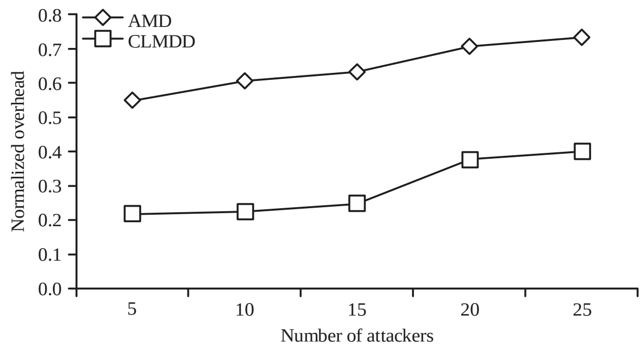

Fig. 5: Normalized overhead for cross-layer based misbehavior detection and defense technique and audit-based misbehavior detection algorithms

Since AMD[10] and hybrid IDS[15] did not handle the misbehavior attacks at MAC layer, more packets were dropped and hence the delivery ratio became low. Since all the nodes were acting as monitoring nodes, the normalized overhead and energy consumption, was increased. Though MAC layer misbehaviors were handled in real-time detection of MAC layer misbehaviors[12], SAMRP[13] and HsF-MAC[14], they did not consider all types of MAC layer misbehaviors into account. Hence the associated packet loss in there schemes were high. The cross-layer based distributed and cooperative IDS[17] and fuzzy based IDS[19] did not involve any strong defense techniques and incur huge computational complexity. Hence the normalized overhead and energy consumption were high in these approaches.

However, the proposed CLMDD technique did not distinguish the packet losses due to regular link errors or due to malicious drop, resulting in more false positives. Hence the future work focuses on developing methodologies for accurately detecting the selective dropping attacks.

CONCLUSION

A CLMDD technique for MANET has been proposed in this paper. In this technique, trusted monitoring nodes are selected using ACO algorithm. The technique consists of receiver detection module and an audit module. In receiver detection module, backoff cheating attack is detected. In audit module, greedy nodes which perform the MAC layer misbehaviors are detected. By simulation results, it has been shown that the CLMDD reduces the packet drop and normalized control overhead with increased packet delivery ratio. Future work concentrates on more attack metrics and related protocols for evaluation.

SIGNIFICANCE STATEMENT

This study covers the detection and prevention of misbehavior detection attacks in MANET that can be beneficial for applications related to mobile communications. This study will help the researchers to uncover the critical areas of misbehaviour attacks on various layers of the protocol stack. Thus a new theory on energy and cost effective IDS may be arrived at.

REFERENCES

1. Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK-A secure intrusion-detection system for MANETs. IEEE Trans. Ind. Electron., 60: 1089-1098.
2. Cardenas, A.A., S. Radosavac and J.S. Baras, 2004. Detection and prevention of MAC layer misbehavior in ad hoc networks. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, October 25-25, 2004, Washington DC, USA., pp: 1722-10.1145/1029102.1029107.
3. Chiejina, E., H. Xiao and B. Christianson, 2015. A dynamic reputation management system for mobile Ad Hoc networks. Computers, 4: 87-112.
4. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 255-265.
5. Khalil, I. and S. Bagchi, 2011. Stealthy attacks in wireless ad hoc networks: Detection and countermeasure. IEEE Trans. Mobile Comput., 10: 1096-1112.
6. Ranjan, A. and R. Selvaraj, 2012. Malicious attacks detection in wireless Ad Hoc networks by using SNDP protocol. http://repository.bothouniversity.ac.bw/buir/bitstream/handle/123456789/37/abhishek%2branjan1.pdf?sequence=1 and isAllowed=y

7. Khan, U., S. Agrawal and S. Silakari, 2015. A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks. In: Information Systems Design and Intelligent Applications, Mandal, J.K., S.C. Satapathy, M.K. Sanyal and P.P. Sarkar (Eds.). Springer, New Delhi, ISBN: 978-81-322-2250-7, pp: 11-19.
8. Nadeem, A. and M.P. Howarth, 2014. An intrusion detection and adaptive response mechanism for MANETs. Ad Hoc Netw., 13: 368-380.
9. Abbas, S., M. Merabti, D. Llewellyn-Jones and K. Kifayat, 2013. Lightweight sybil attack detection in MANETs. IEEE. Syst. J., 7: 236-248.
10. Zhang, Y., L. Lazos and W. Kozma, 2016. AMD: Audit-based misbehavior detection in wireless ad hoc networks. IEEE Trans. Mobile Comput., 15: 1893-1907.
11. Kozma, Jr. W. and L. Lazos, 2008. Reactive identification of misbehavior in ad hoc networks based on random audits. Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 16-20, 2008, San Francisco, CA, USA., pp: 612-614.
12. Aaroud, A., M.A. El Houssaini, A. El Hore and J. Ben-Othman, 2017. Real-time detection of MAC layer misbehavior in mobile ad hoc networks. Applied Comput. Inform., 13: 1-9.
13. Arthur, M.P. and K. Kannan, 2015. Intelligent internal stealthy attack and its countermeasure for multicast routing protocol in MANET. ETRI J., 37: 1108-1119.
14. Djahel, S., Z. Zhang, F. Nait-Abdesselam and J. Murphy, 2012. Fast and efficient countermeasure for MAC layer misbehavior in MANETs. IEEE Wireless Commun. Lett., 1: 540-543.
15. Subba, B., S. Biswas and S. Karmakar, 2016. Intrusion detection in mobile Ad-hoc networks: Bayesian game formulation. Eng. Sci. Technol. Int. J., 19: 782-799.
16. Khan, M.S. and N.M. Khan, 2016. Low complexity signed response based sybil attack detection mechanism in wireless sensor networks. J. Sens., Vol. 2016. 10.1155/2016/9783072.
17. Vali, Y.S. and T.R. Rangaswamy, 2017. An efficient cross-layer based intrusion detection system for mobile Ad Hoc networks. J. Theor. Applied Inform. Technol., 95: 47-58.
18. Imani, M., M.E. Rajabi, M. Taheri and M. Naderi, 2015. A novel approach to combine misuse detection and anomaly detection using POMDP in mobile Ad-Hoc networks. Int. J. Inform. Electron. Eng., 5: 245-249.
19. Balan, E.V., M.K. Priyan, C. Gokulnath and G.U. Devi, 2015. Fuzzy based intrusion detection systems in MANET. Procedia Comput. Sci., 50: 109-114.
20. Grover, J., M.S. Gaur and V. Laxmi, 2015. Multivariate verification for sybil attack detection in VANET. Open Comput. Sci., 5: 60-78.
21. Mangla, A. and Vandana, 2015. Detection of physical jamming attacks in MANETs. Int. J. Sci. Eng. Technol. Res., 4: 1972-1976.
22. Justus, J.J. and A.C. Sekar, 2013. A fault tolerance data aggregation scheme for wireless sensor networks. Int. Rev. Comput. Software, 8: 1556-1563.
23. Paranjape, S. and M. Sutaone, 2013. A cluster based routing protocol with mobility prediction for mobile sensor networks. Int. Rev. Comput. Software, 8: 2614-2623.