http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

OPEN ACCESS Information Technology Journal

ISSN 1812-5638
DOI: 10.3923/itj.2016.84.90

Research Article
Harmony Search Algorithm to Prevent Malicious Nodes in Mobile Ad Hoc Networks (MANETs)

Ahmed Mohammed Fahad and Ravie Chandren Muniyandi

Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Abstract

Background: Security is widely acknowledged as a critical problem when implementing mobile ad hoc networks (MANETs) given that these networks are vulnerable to routing attacks. Although, providing authentication to the packets at each stage can reduce the risk, MANETs are still vulnerable to such attacks due to the time delay in reporting and analyzing of packets. Therefore, this problem needs further exploration and study to provide an increasingly robust and efficient solution. **Materials and Methods:** To overcome this problem, this study modified the Chang scheme using the Harmony Search Algorithm (HSA). Data for the study were simulated and analyzed using MATLAB. **Results:** Results showed that the HSA had a relatively better packet delivery ratio compared with Dynamic Source Routing (DSR) and Cooperative Bait Detection Scheme (CBDS). The HSA routing protocol achieved 30 and 83% compared with DSR and CBDS, respectively. In addition, a 0.76 and 0.89% routing overhead was achieved by HSA compared with DSR and the CBDS, respectively and the end-to-end delay for HSA was 0.07 and 0.49% compared with DSR and CBDS, respectively. **Conclusion:** In sum, the study findings imply that HSA performs better than CBDS and DSR.

Key words: Dynamic source routing, cooperative bait detection scheme, harmony search algorithm, blackhole attack

Received: May 10, 2016 Accepted: May 30, 2016 Published: June 15, 2016

Citation: Ahmed Mohammed Fahad and Ravie Chandren Muniyandi, 2016. Harmony search algorithm to prevent malicious nodes in mobile ad hoc networks (MANETs). Inform. Technol. J., 15: 84-90.

Corresponding Author: Ahmed Mohammed Fahad, Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

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

The mobile devices that can configure themselves into ready-to-use devices without depending on any physical infrastructure are referred to as mobile ad hoc networks (MANETs)[1]. The MANETs comprise mobile devices, such as laptops, personal computers, mobile phones, MP3 players and personal digital assistant devices, which move freely both inside and outside the network[2].

The MANETs are established by the internet engineering task force, which ensures that the internet protocol routing protocols are well developed[3]. Routing protocols have been the focus of a substantial number of study[4]; hence, numerous protocols have been developed because of MANETs.

The security of MANETs is important because it assures the presence of network services, integrity and confidentiality of data[5]. Frequent security attacks on MANETs are usually caused by several factors, such as open medium features, changes in dynamic topology, absence of central management, lack of clear defense mechanisms and cooperative algorithms[6]. The MANETs consider security of information as the most critical element. In this event, secure communication and information transmission have to be strictly observed and protected from attackers. Security information and transmission engineers must be conversant with all possible methods of attacks.

Examples of attacks that can be launched to MANETs include the blackhole attack, wormhole attack, selfish device misbehavior, Sybil attack, routing table overflow attack, flooding attack, impersonation attack and Denial of Service[7]. The MANETs are significantly vulnerable to such attacks because of information exposure resulting from mutual trust of communication between devices[8].

Accordingly, engineers should understand the side effects associated with the exposure of information in MANETs. Secured MANETs should assure security and eliminate the daily fears of insecurity[9].

The security weakness of a MANET makes it a potential destination for routing attacks[10]. For example, a blackhole attack on a MANET modifies its routing function, thereby exposing it to abnormal packet transfers[11]. A blackhole attack can access and propagate through the network in an unauthorized manner[12]. Figure 1 shows a typical scenario of a blackhole attack.

This technique compromises the network performance to provide security without overloading the network heavily. Such approach can help monitor the spatial-time behavior of MANETs along with performance, topography and network security. However, this particular method may be exposed to further attacks during data transmission given that a malicious node may become active and may mislead the detection process. Providing authentication to the packets at each stage can overcome this issue to a certain extent. Nevertheless, routing attacks may still succeed because a time delay in reporting and analyzing of packets may have already transmitted them to malicious nodes. Therefore, this problem needs further exploration and study to attain an increasingly robust and efficient solution.

This study aimed to mitigate this delay by modifying the Chang *et al.*[14] approach, which opposes the collaborative attacks by malicious nodes in MANETs using the HSA.

MATERIALS AND METHODS

The HSA is inspired by music; it is an evolutionary algorithm that mimics the process of improvisation, which is widely used by music players. This algorithm provides easy

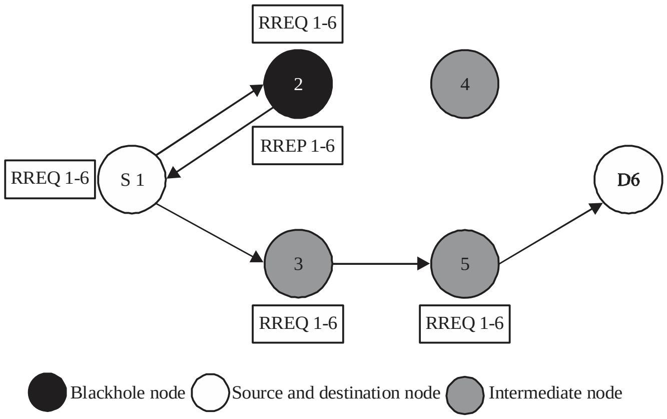
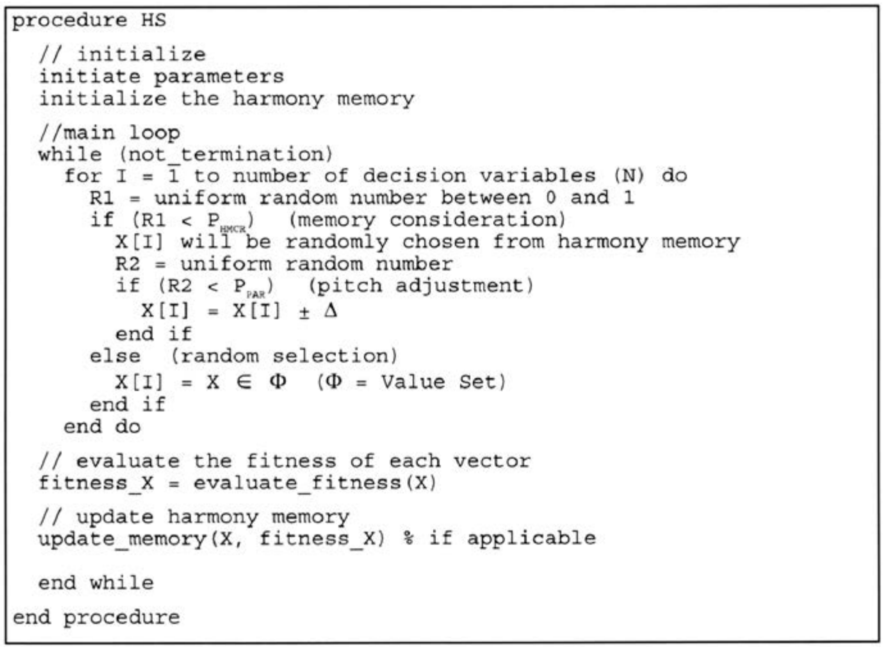


Fig. 1: Blackhole attacks[13]



```
procedure HS
  // initialize
  initiate parameters
  initialize the harmony memory
  //main loop
  while (not_termination)
    for I = 1 to number of decision variables (N) do
      R1 = uniform random number between 0 and 1
      if (R1 < $P_{HMCR}$)  (memory consideration)
        X[I] will be randomly chosen from harmony memory
        R2 = uniform random number
        if (R2 < $P_{PAR}$)  (pitch adjustment)
          X[I] = X[I] ± Δ
        end if
      else  (random selection)
        X[I] = X ∈ Φ  (Φ = Value Set)
      end if
    end do
  // evaluate the fitness of each vector
  fitness_X = evaluate_fitness(X)
  // update harmony memory
  update_memory(X, fitness_X) % if applicable

  end while
end procedure
```

Source: Advances in Evolutionary Algorithms, Book edited by: Witold Kosiński, ISBN 978-953-7619-11-4, pp. 468, November 2008, I-Tech Education and Publishing, Vienna, Austria

Fig. 2: Pseudocode of HSA[18]

implementation and is based on a simple concept[15]. In addition, the simulation in this algorithm involves only a few parameters given that its theory is based on stochastic derivative[16]. The HSA was initially developed for discrete optimization, but was eventually used for continuous optimization[17]. Figure 2 shows the step-by-step pseudocode of HSA.

Previous approach: Chang *et al.*[14] designed and tested cooperative bait proactive scheme (CBDS) based on Dynamic Source Routing (DSR)[14]. The results in this previous study showed that CBDS performs better than DSR, best effort fault tolerant (BFTR) and 2ACK protocols[19]. For example, CBDS provides a higher Packet Delivery Ratio (PDR) than BFTR, 2ACK and DSR. In addition, CBDS gives a higher throughput than DSR for all simulation cases. Nonetheless, the 2ACK scheme was determined capable of providing the highest routing overhead compared with CBDS, BFTR and DSR. This observation was noted irrespective of the number of malicious nodes[20]. Chang concluded that CBDS is an efficient scheme in terms of routing overhead and PDR.

HSA for MANET enhancement: This study proposes the use of HSA to reduce the delay in malicious node detection techniques such as the CBDS. Such application can help detect and prevent blackhole attacks, which launch malicious nodes in MANETs. This scheme can also help the source node select a neighboring node that will work in tandem to identify the bait destination for a malicious node, which will then send a Route REPly (RREP) message as a response. Therefore, this scheme uses reverse tracing to identify and prevent malicious nodes, thereby helping launch an alarm in the network when the system observes a significant drop in the PDR. In turn, this alarm launches a malicious node detection mechanism to prevent false nodes.

The DSR is the base for CBDS. Although it traces all the node addresses used during the routing path (i.e., from source to destination), DSR may provide no information to the source node to differentiate between the malicious node (false RREP) and true node reply. This occurrence may misdirect the source node, which may send packets through the false shortest route advertised by the malicious nodes. This scheme adds a HELLO message to the CBDS to facilitate and identify its true neighboring node and traverse the subsequent node in the range of one hop. This function further uses the proposed HSA-CBDS scheme to send a test bait in the form of address to identify and eliminate the malicious nodes. These Route REQuest (RREQ) baits are extremely similar to the true RREQ

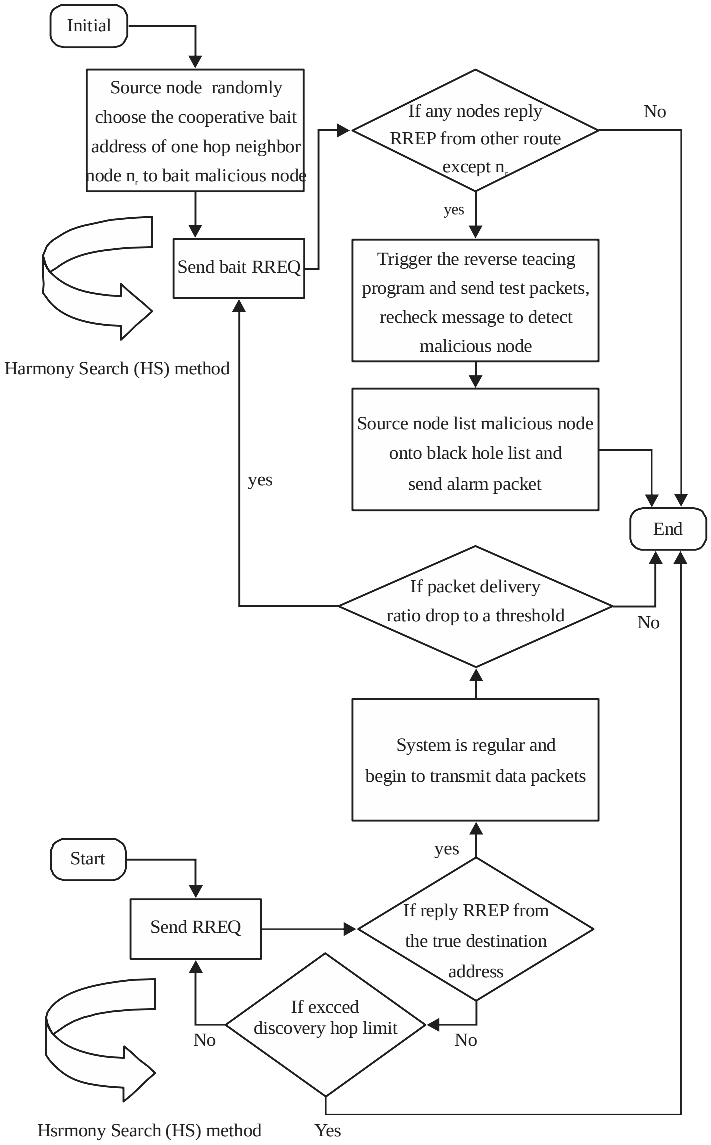

Initial
Source node randomly choose the cooperative bait address of one hop neighbor node n_r to bait malicious node
Send bait RREQ
Harmony Search (HS) method
If any nodes reply RREP from other route except n_r
No
yes
Trigger the reverse teacing program and send test packets, recheck message to detect malicious node
Source node list malicious node onto black hole list and send alarm packet
yes
End
If packet delivery ratio drop to a threshold
No
System is regular and begin to transmit data packets
yes
Start
Send RREQ
If reply RREP from the true destination address
If excced discovery hop limit
No
No
Hsrmony Search (HS) method
Yes

Fig. 3: Proposed algorithm

packets with the only difference of being intended to identify the address of a malicious node.

Three rules mentioned below need to be followed:

- Always play any single pitch from the available method, which will be HSA-CBDS
- Play neighboring pitch HSA-CBDS with the scheme proposed by Chang *et al*.[15] (i.e., threshold value)
- All possible CBDS ranges play a random pitch (i.e., this process mimics the selection of each variable for the HSA)

The following additional rules should be implemented as well:

- Select a random value from the memory of HSA (i.e., from the random vector)
- Select a neighboring value for the memory of HSA
- Choose a random value from the possible value range

The discussion in the preceding paragraph states that an objective function with HSA memory should be formulated to help enhance the Chang scheme (i.e., improve the end-to-end traversal time).

Methodology design: While, in Fig. 3 shows the propped algorithm flowchart process and in Table 1 presents the parameters considered for the analysis and simulation through MATLAB 2015a.

Table 1: Simulation parameters

Parameters	Value
Application traffic	10 CBR
Transmission rate	4 packets/sec
Radio rage	250 m
Packet size	512 bytes
Channel data rate	11 Mbps
Pause time	0 sec
Maximum speed	20 m sec^{-1}
Simulation time	800 sec
Area	700×700 m
Malicious nodes	0-40%
Number of nodes	50
Threshold	Dynamic threshold
PDR	Packet delivery ratio
Throughout	$\frac{\sum \text{Packets received by destination}}{\text{Stop time} - \text{Start time}}$
Routing overhead	It shows the data being lost
End-to-End Delay	Time the data travels between host

RESULTS AND DISCUSSION

Results have been compared with six related works in addition with the base paper that we have investigated the delay. As it can shown in Nandhini *et al*.[21] scheme their routing transparency by CBDS is low performance in term of the comparison with our enhanced results in PDR. While in Ramya and Mylsamy[22] study they only investigate their result in just two metrics -which are throughput and packet loss. While, our finding lies more in routing overhead and end to end delay. This study based on HAS , which is better of ant colny optimization for reducing the black-hole attack as Kaur and Kaur[23] results due to the ACO disadvantage of sequences of random decisions. The other impressive finding study that our end to end delay is better than DJKLJKL model[24]. Whereas DJKLJKL shown a leak in their end to end delay. The drawback of Singh *et al*.[25] well seen in their performance and security issue as well. In Chauhan *et al*.[26] use selfish nodes use the services of network but do not provide services like packet forwarding, to the network. They provide a acceptable level of security, but in term of efficiency they leak on a battery power, memory, bandwidth and CPU time which is mitigated in this study[26].

Figure 4 shows the variations in the PDR of the three routing protocols, namely, HSA, DSR and CBDS. The HSA decreased from 0.9962-0.9640 when the malicious node ratio was varied with the introduction of three malicious nodes in the network. Similarly, DSR decreased from 0.8571-0.5714 and the CBDS decreased from 1.000-0.6667. However, the HSA had a relatively better PDR compared with DSR and CBDS. The HSA routing protocol achieved 14 and 80% in comparison with DSR and CBDS protocols, respectively.

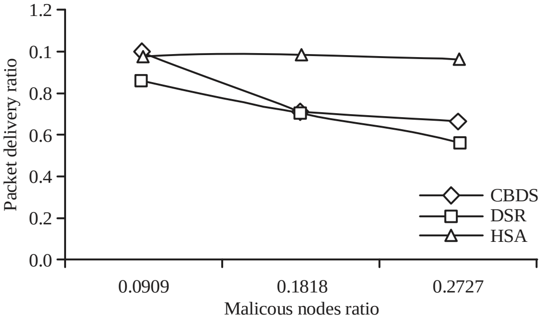


Fig. 4: Variations in PDR

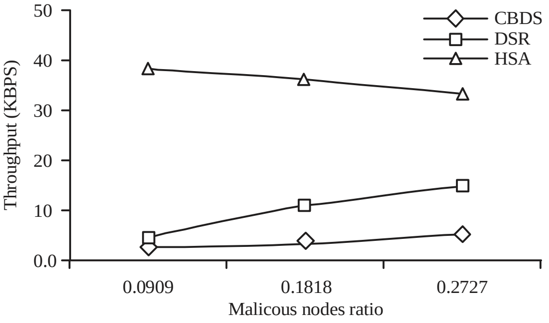


Fig. 5: Variations in throughput

The HSA protocol achieved a better PDR, indicating that no packets were lost during transmission. The packets reached their destinations without any loss because the route once established was maintained correctly. The PDR values of the HSA also indicated that no or miniscule retransmissions were required to indirectly help attain high throughputs.

Figure 5 presents the variations in throughputs of the three routing protocols investigated in this study when the malicious node ratio varies with the introduction of three malicious nodes in the network. The throughput for the HSA decreased from 38.3-33.5 kbps, but increased from 5.13-14.8 kbps for DSR and from 2.5-5.4 kbps for CBDS. Among these protocols, the HSA showed the best throughput. The HSA routing protocol achieved 30 and 83% compared with the DSR and CBDS protocols, respectively.

Therefore, HSA can achieve better throughputs compared with the DSR and CBDS algorithms. According to the HSA protocol, packets reach their destinations without any delay and loss. Hence, the channel's bandwidth is utilized efficiently, leading to increased throughputs.

Figure 6 presents the variations in the routing overhead of the three routing protocols when the malicious node ratio

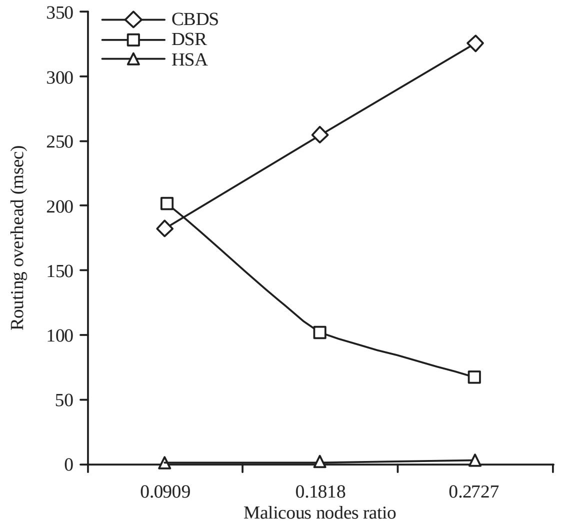


Fig. 6: Variations in routing overhead

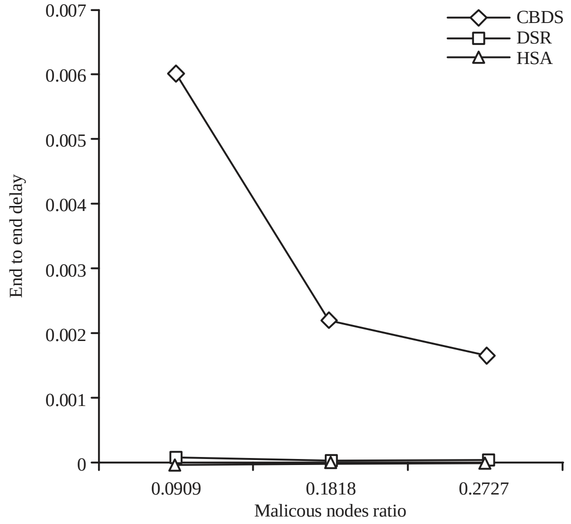


Fig. 7: Variations in end-to-end delay

is varied. The decrease in HSA and DSR was from 1.99-3.6 msec and from 204.1-68 msec, respectively. Contrarily, the routing overhead in CBDS increased from 183.7-326.5 msec. The HSA routing overhead was relatively better than that of DSR and CBDS. The HSA routing protocol achieved 0.76 and 0.89% compared with the DSR and CBDS protocols, respectively.

The results of the HSA protocol for routing overhead indicate that the overhead for any retransmission is reduced for packets compared with DSR and CBDS. The route established by the protocol is maintained efficiently, resulting in reduced end-to-end delay with high PDR and high throughput. This well-established route requires minimal retransmissions for any segments if found missing, thereby reducing the routing overhead.

Figure 7 shows the variations in end-to-end delay of the three routing protocols. When the malicious node ratio was varied with the introduction of three malicious nodes in the network, the HSA decreased from 5.22×10^{-7} to 1.47×10^{-7}, the DSR decreased from 9.7×10^{-5} to 3.24×10^{-5} and the CBDS decreased from 0.0060-0.0016. However, the HSA showed a relatively better PDR compared with DSR and CBDS. The HSA routing protocol achieved 0.07% compared with the DSR protocol and 0.49% compared with the CBDS protocol.

The results of the HSA protocol for end-to-end delay suggest that the time taken for the packets to transfer from source to destination is less compared with DSR and CBDS. The time recorded is also less given that the time for route discovery at each node is less likely to result in an overall decrease in the total end-to-end delay.

This study used a music improvisation technique to search for an efficient harmony by testing and employing a set of combinations (i.e., different pitches). This study primarily aimed to propose and maximize the ratio for detecting and preventing malicious nodes that launch gray hole/collaborative blackhole attacks in a network. This study intends to provide an increasingly robust technique or scheme for protecting packets (i.e., communication of nodes in MANETs). Improved schemes for protecting MANETs from attacks should be established and implemented. The literature review indicated that an ad hoc network is highly vulnerable to different types of attacks in MANETs due to its dynamic topology and lack of any authentication system.

CONCLUSION

This study proposes the use of HSA to reduce the delay in CBDS. Such an approach can help detect and prevent blackhole attacks, which launch malicious nodes in MANETs. This scheme can also help the source node select a neighboring node that will work in tandem to identify a bait destination for a malicious node, which will then send a RREP message in reply. The spurring result shows improvement in the delay, throughput, PDR, end-to-end delay and routing overhead. This scheme adopts reverse tracing to identify and prevent malicious nodes based on HSA.

ACKNOWLEDGEMENT

This study was supported by Dana Impak Perdana (DIP-2014-037) of the Universiti KebangsaanMalaysia (UKM).

REFERENCES

1. Yi, Y., S. Lee, W. Su, M. Gerla and A.C. de Verdiere, 2014. On-demand multicast routing protocol (ODMRP) for Ad Hoc networks. Mobile Ad Hoc Networking (MANET) Internet-Draft, University of California, Los Angeles. http://ftp.uni-siegen.de/drafts/draft-gerla-manet-odmrp-02.pdf
2. Veni, R.M. and R. Latha, 2013. Mobile ad hoc network. Int. J. Sci. Res., 2: 74-79.
3. Chen, Y.S., C.S. Hsu and C.H. Cheng, 2014. Network mobility protocol for vehicular ad hoc networks. Int. J. Commun. Syst., 27: 3042-3063.
4. Taneja, S. and A. Kush, 2010. A survey of routing protocols in mobile adhoc networks. Int. J. Innovation Manage. Technol., 1: 279-285.
5. 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.
6. Akbani, R., T. Korkmaz and G. Raju, 2012. Mobile Ad-Hoc Networks Security. In: Recent Advances in Computer Science and Information Engineering, Qian, Z., L. Cao, W. Su, T. Wang and H. Yang (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-642-25768-1, pp: 659-666.
7. Jhaveri, R.H., S.J. Patel and D.C. Jinwala, 2012. DoS attacks in mobile ad hoc networks: A survey. Proceedings of the 2nd International Conference on Advanced Computing and Communication Technologies, January 7-8, 2012, Rohtak, Haryana, pp: 535-541.
8. Ullah, I. and S.U. Rehman, 2010. Analysis of black hole attack on MANETs using different MANET routing protocols. School of Computing Blekinge Institute of Technology, Sweden.
9. Pathan, A.S.K., 2010. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. Auerbach Publications, USA.
10. Goyal, P., V. Parmar and R. Rishi, 2011. MANET: Vulnerabilities, challenges, attacks, application. Int. J. Comput. Eng. Manage., 11: 32-37.
11. Mishra, A., R. Jaiswal and S. Sharma, 2013. A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc network. Proceedings of the IEEE 3rd International Advance Computing Conference, February 22-23, 2013, Ghaziabad, pp: 499-504.
12. Bawa, K. and S.B. Rana, 2015. Prevention of black hole attack in MANET using addition of genetic algorithm to bacterial foraging optimization. Int. J. Curr. Eng. Technol., 5: 2406-2411.
13. Tseng, F.H., L.D. Chou and H.C. Chao, 2011. A survey of black hole attacks in wireless mobile ad hoc networks. Hum.-Centric Comput. Inform. Sci., Vol. 1. 10.1186/2192-1962-1-4
14. Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J., 9: 65-75.
15. Assad, A. and K. Deep, 2016. Applications of Harmony Search Algorithm in Data Mining: A Survey. In: Proceedings of Fifth International Conference on Soft Computing for Problem Solving, Pant, M., K. Deep, J.C. Bansal, A. Nagar and K.N. Das (Eds.). Springer, Singapore, ISBN: 978-981-10-0450-6, pp: 863-874.
16. Geem, Z.W., 2008. Novel derivative of harmony search algorithm for discrete design variables. Applied Math. Comput., 199: 223-230.
17. Lee, K. and Z. Geem, 2005. A new meta-heuristic algorithm for continuous engineering optimization: harmony search theory and practice. Comput. Methods Applied Mechanics Eng., 194: 3902-3933.
18. Alatas, B., 2010. Chaotic harmony search algorithms. Applied Math. Comput., 216: 2687-2699.
19. Wankhade, S.V., 2012. 2ack-scheme: Routing misbehavior detection in manets using olsr. Int. J. Sci. Eng. Technol. Res., 1: 1-7.
20. Arya, P., G.P. Negi, P.K. Dhiman and K. Kapoor, 2015. CBDS (Cooperative bait detection scheme) ATTACK-a review. Int. J. Adv. Res. Comput. Eng. Technol., 4: 3428-3434.
21. Nandhini, M., J. Sathya, T. Sundaridevi, G. Sivaprakash, J. Jaya and P. Premalatha, 2016. Detecting and preventing malicious nodes using cooperative bait detection scheme. Front. Curr. Trends Eng. Technol., 1: 28-36.
22. Ramya, V. and S. Mylsamy, 2016. Removal of malicious nodes launching blackhole attack in MANETs. Wireless Commun., 8: 6-10.
23. Kaur, H. and H. Kaur, 2016. The approach for the prevention of black hole attack in MANET using DSR protocol and ant colony optimization technique: A review. IITM J. Manage. IT, 7: 8-11.
24. Haghighi, A., K. Mizanian and G. Mirjalily, 2015. Modified CBDS for defending against collaborative attacks by malicious nodes in MANETs. Proceedings of the 2nd International Conference on Knowledge-Based Engineering and Innovation, November 5-6, 2015, Tehran, pp: 902-907.
25. Singh, U.K., J. Patidar and K.C. Phuleriya, 2015. On mechanism to prevent cooperative black hole attack in mobile Ad Hoc networks. Int. J. Scient. Res. Comput. Sci. Eng., 3: 11-15.
26. Chauhan, A., D.K. Gupta and M.K. Sah, 2015. Detection of packet dropping nodes in MANET using DSR routing protocol. Int. J. Comput. Applic., 123: 10-16.