International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 3 (June 2016), pp.150-162

http://www.meacse.org/ijcar

Enhanced Packet Dropping Algorithm and Neighbour Node Cluster Strategy for Intrusion Detection in MANET

E.Selvi[1] and M.S. Shashidara[2]

[1]Department of Computer Science, Asan Memorial College of Arts and Science, Chennai, India
[2]Department of MCA, The Oxford College of Engineering, Bangalore, India

Abstract

In MANET, every mobile node acts as both a transmitter and a receiver via bidirectional wireless links without requirements of any fixed network infrastructure. Intrusion-detection mechanisms effectively protect MANET from attacks using pre-distributed keys. Many intrusion detection systems were developed for MANET to improve the security level and to detect the malicious attackers in the network. However malicious node identification and their subsequent isolation from network and problems posed due to pre-distributed keys remained unsolved, compromising securing and therefore increasing the routing overhead. In this research work an Intrusion Detection technique to detect the malicious node by providing better security and reducing the routing overhead called Integrated Cluster and Highest Connectivity-based Packet Dropping (IC-HCPD) for mobile ad hoc network is presented. Neighbor Node-based Cluster Formation is designed in the proposed IC-HCPD technique aiming at reducing the routing overhead by obtaining the route using minimal distance. Consequently, the neighbor node possessing highest connectivity is selected as the Detection Manager using Cluster algorithm based on Highest Connectivity. Finally, the Detection Manager monitors the nodes entering into and leaving the network and identifies the faulty node and isolates the node from the network through Packet Dropping mechanism. The simulation results show that IC-HCPD technique can effectively improve average packet delivery ratio, reduces routing overhead for data delivery, and improves security as compared with those of the tested algorithms.

Keywords: Mobile ad hoc network, malicious node, pre-distributed keys, Highest Connectivity, Packet Dropping

1. Introduction

Due to the inherent vulnerabilities of mobile ad hoc networks, new intrusion detection measures need to be developed to efficiently safeguard the route from further being deteriorated. This work focuses on the detection of intruder nodes and isolating them from the network. Identity of polluters in MANET was identified [1] by applying a fully distributed technique with low computational overhead. In [2] enhanced adaptive acknowledgement model was introduced to improve the malicious node detection behavior rate. A virtual clustering [3] model was applied in heterogeneous network to improve the packet forwarding rate in the presence of malicious nodes. Another distributed technique [4], called as encounter-based distribution algorithm to detect the malwares with the aid of content-based signature was presented. Link state routing [5] is an efficient method to detect malicious node and isolate them from the network, so that the network does not get further disrupted. Surveying adjacent nodes was another mechanism used in [6] that resulted in minimizing the false alarm and also sending and checking packet for neighbor nodes being transmission.

Adaptive distribution mechanism for intrusion detection has been used for a long time [7]. This technique introduced a flexible responsive scheme in various attack scenarios with low network overhead. Evaluation of classification algorithms to detect malicious activities in MANET and their comparison results was presented in [8].

Intrusion detection systems were used in the past by several researchers using different methods to detect intrusions in networks in an efficient manner. However, most of these methods only detected the intruders only with high false alarm rate. Intelligent Agent intrusion detection model [9] was presented by integrating attribute selection, outlier detection, and enhanced multiclass SVM classification methods to detect anomalies with low false alarm rate. But, with the increase in the congestion rate, intrusion model did not work efficiently.

In this paper we propose a new intrusion detection method which is called Integrated Cluster and Highest Connectivity-based Packet Dropping (IC-HCPD). This method detects the malicious node with the help of the detection manager. The detection manger on the other hand based on the neighbor information performs clustering and detects the intruder or malicious node through packet dropping mechanism and isolates the node from the network. Consequently, routing overhead is decreased whereas the packet delivery ratio malicious node detection behavior rate is increased considerably in this method.

The rest of this paper is organized as follows: Section 2 presents a brief introduction of related works. Section 3 proposes our Integrated Cluster and Highest Connectivity-based Packet Dropping (IC-HCPD) method. In Section 4 the simulation results will be described. Finally Section 5 concludes our discussion.

2. Background and related work

Some recent studies have examined and discussed the problem of intrusion detection methods in mobile ad hoc network. Some of them will be surveyed in this section. An integrated cultural algorithm and artificial fish swarm algorithm [13] for anomaly detection of nodes was presented using optimized back propagation model. In [14], KNN classification algorithm was applied which detected the intrusion with high detection rate that separated normal nodes from abnormal nodes in purview of identifying the intruder nodes.

In [15], a new algorithm for preventing the network against jamming attack strategies using heuristic algorithm was designed. In [16], intrusion rate was reduced by protecting the location privacy using steiner tree aiming at improving the privacy and reducing the communication cost substantially. In [17], a framework for wireless mesh networks was designed using cooperative cross layer framework.

In [18], non parametric cumulative sum was used to detect the rate of intrusion against cognitive radio networks. By learning the normal operational model, the proposed intrusion detection system was able to detect anomalous or abnormal behavior arising from an attack. Attacks may also arise due to resource depletion. In [19], routing protocol layer was investigated to measure the VAMPIRE attacks through network wide energy usage

All of the above said methods perform intrusion detection by either compromising the security when providing routing overhead and vice versa. In this paper we propose a new algorithm that performs intrusion detection by identifying the malicious node and isolating the node from the network.

3. Proposed Intrusion Detection technique

In this section, first the problem statement is described, then the novel strategy for intrusion detection in MANET is proposed and finally the Neighbor Node-based Cluster Formation and Highest Connectivity-based Detection Manager strategies are presented.

3.1 Problem statement

The nodes in MANETs assume that other nodes seldom cooperate with each other to relay data, which is exploited by malicious nodes and propagate intrusive attacks across the network. The mobile nodes in MANET change the topology at a faster rate resulting in the increase in routing overhead.

With autonomous collection of mobile nodes, intrusion detection is one of the major topics being analyzed in Mobile Ad hoc Network. Distributed techniques were employed to infer the identity of malicious nodes and digital signature were applied to demonstrate higher malicious behavior detection rates.

However, conventional distributed techniques cannot isolate the malicious node and with the random nature of the network application of pre-distributed key pattern, increases the routing overhead substantially.

In our technique, we consider MANET as an undirected graph '$G = (V, E)$', with transmission range 'R' where 'V' represents the set of nodes and 'E' represents the set of bidirectional links. However, due to the presence of intruders that utilize the loophole to carry out the malicious behavior and therefore nodes gets compromised and more data packets cannot be successfully delivered to destinations.

The cluster head or detection manager selection is invoked on-demand in the proposed technique, and is aimed to reduce the routing overhead and therefore the communication costs. By classifying the mobile nodes in the network into clusters, the proposed technique allows the Detection Manager (DM) to identify the faulty node and isolate the node from the network. To achieve the goal of intrusion detection of malicious nodes in MANET, in the presence of malicious node, this paper design an intrusion detection technique where detection manager detect the malicious node and improve the packet delivery ratio and reduces the routing overhead using clustering technology.

3.2 Neighbor Node-based Cluster Formation

In this section, a Neighbor Node-based Cluster Formation is designed aiming at reducing the routing overhead and transmitting data packets in an intrusion free model. Fig 1 shows an example of Neighbor Node-based Cluster Formation for the selection of intermediate nodes.

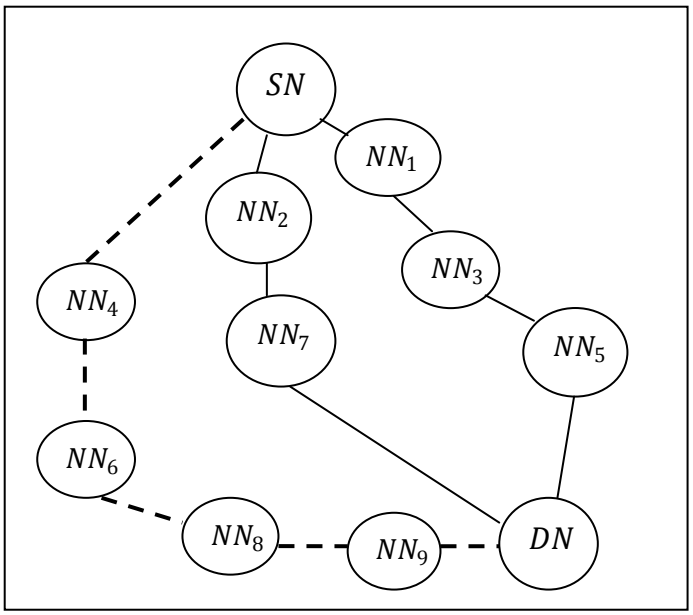

Fig.1 An example selection of intermediate nodes

As shown in fig 1, the source node is denoted as 'SN' and destination node by 'DN'. Nine Neighbor Nodes '$NN_1 - NN_7$' exists between the source destination pair. Normal lines indicate the possible neighbor nodes through which routing can be proceeded whereas the dashed bold line denotes the final neighbor nodes selected through which transmission is forwarded.

In the proposed technique, the intermediate nodes from the source node 'SN' within the transmission range 'R' is measured to ensure secure routing through which data packets are transmitted and is formulated as given below.

$$IN = \sum_{i=1}^{n} Min\left(Dis\ (SN - NN_i)\right) \quad (1)$$

From (Eq.1), the distances between the source node and the neighbor nodes is first evaluated. Then, based on the result obtained, the minimum distance nodes are then selected as the intermediate nodes. If

more than one mobile node possesses similar minimal distance, then the residual distance is used as a basis to obtain the intermediate nodes and is formulated as given below.

$$IN = \sum_{i=1,j=2}^{n} Min\ ResidualDis(NN_i - NN_j) \quad (2)$$

In this way, by measuring the intermediate nodes, Neighbor Node-based Cluster Formation reduces the routing overhead and therefore minimizes the communication cost.

3.3 Highest Connectivity-based Detection Manager Selection

To achieve better packet delivery ratio, we need to keep track of the normal and malicious nodes to accordingly predict which route can be accessed through for packet or file transmission in the near future. With the intermediate nodes obtained using Neighbor Node-based Cluster Formation, the next step in the proposed technique is the identification of Detection Manager (DM). Every mobile node in MANET transmits or receives the data. The task of detection manager in the proposed work is to monitor the nodes which is entering and leaving the network and also identify the malicious node and isolate the node from the network.

In this work, a clustering algorithm based on highest connectivity or with maximum number of neighbors is selected as the cluster head or the Detection Manager (DM). In order to construct highest connectivity clustering, the node degree is measured on the basis of its' (i.e. source mobile node) distance from other mobile nodes in the network. Each mobile node broadcasts its id (i.e. Mobile ID) to the nodes that are within its transmission range 'R'. The structure of the broadcast information is as given below.

$Mobile\ ID$	NN	NM	$Weight_{NN}$	$Weight_{NM}$

Fig 2 Broadcast Information

In order to measure the highest connectivity, the proposed technique obtains two parameters for selecting cluster head or detection manager along with the mobile node ID '$Mobile\ ID$' namely, neighbour node information 'NN' and node mobility 'NM' (as listed in fig 2). The neighbour node information comprises of the weight of neighbouring node '$Weight_{NN}$' present in its vicinity or transmission range 'R'.

On the other hand, the weight of the node mobility '$Weight_{NM}$' symbolizes the mobility of the nodes in network that depends upon the mobility pattern. Initially, the values of '$Weight_{NN}$' and '$Weight_{NM}$' are set to 0. With changes in the updates, the two values are incremented. These two parameters (values) along with the mobile node ID are used to measure the node capability. With this node capability, the mobile node that possesses high capability is selected as the cluster head or the detection manager 'DM_i'.

$$DM_i = Max\ \sum_{i=1}^{n}(Weight_{NN}[IN] + Weight_{NM}\ [IN]) \quad (3)$$

From (Eq.3), the mobile node with maximum number of neighbors (i.e., maximum degree) is selected as the cluster head or detection manager. Mobile node possessing highest connectivity is considered as the detection manager.. If two or more intermediate nodes possess the same capability, then the residual distance is used as given below.

$$DM_i = Min\ ResidualDis\ (Max\ \sum_{i=1}^{n}(Weight_{NN}[IN] + Weight_{NM}[IN])) \quad (4)$$

From (Eq.4), based on the minimum residual distance, detection manager is identified in the presence of more than one DM. By effective detection of DM, packet delivery ratio is improved significantly.

Input: Mobile ID '$Mobile\ ID$', Neighbor Node 'NN', Node Mobility 'NM', weight neighbouring node '$Weight_{NN}$', weight node mobility '$Weight_{NM}$', Source Node 'SN', Destination Node 'DN', Intermediate Node '$IN_1 - IN_7$',
Output: optimizes packet delivery ratio and reduces routing overhead
1: Begin 2: Set '$Weight_{NM}$', $Weight_{NN}$' to be 0 3: For each Source Node 'SN' and Destination Node 'DN' 4: Repeat 5: Measure Intermediate Nodes using (1) 6:if (more than one intermediate nodes obtained) 7:Measure Intermediate Nodes based on residual distance using (2) 8:End if 9: Until (Intermediate Nodes are obtained) 10: Obtain Detection Manager using (3) 11: If (more than one Detection Manager is obtained) 12:Measure Detection Manager based on residual distance using (4) 13: End if 14:End for 15: End

Fig 3 Clustering algorithm based on Highest Connectivity

As shown in the fig 3, for each source destination pair, whenever a source node has to identify the best route to forward packets in MANET, intermediate nodes are measured. In the presence of more than one intermediate node minimum residual energy is used. Followed by this, the identification of detection manager is performed based on the highest connectivity. The highest connectivity or the maximum number of neighbors possessed by the intermediate nodes is then identified as the detection manager.

3.4 Packet Dropping-based Malicious Node Isolation model

Finally, Packet Dropping-based Malicious Node Isolation strategy aiming at improving the security is presented. As implied by the name, the detection manager in the network isolates the malicious node from communicating with other nodes in the network. In turn, this prevents the victim node from receiving data packets from other mobile nodes in the network.

The idea behind Packet Dropping-based Malicious Node Isolation strategy is that the link information is prevented from being spread to the entire network. As a result, these nodes will not be able to build a route to these target nodes. This attack is achieved by exploiting the Detection Manager Neighbor Node Relay Selection (DMNNRS) algorithm.

Each mobile node selects a set of its neighbor nodes 'NN'. Only nodes, selected as 'NN' by the Detection Manager 'DM', are responsible for identifying the faulty node and isolate the node from the network. Fig 4 shows the DMNNRS algorithm.

Input: Mobile Node '$MN_i = MN_1, MN_2, \dots, MN_n$', Neighbor Node '$NN_i = NN_1, NN_2, \dots, NN_n$', Packet '$P_i = P_1, P_2, \dots, P_n$'
Output: Improves security and malicious node behavior detection rate
1: Begin 2: For each Mobile Node 'MN_i' 3: Measure set of its neighbor nodes 'NN' 4: Obtains packets 'P_i' from its Neighbor Node 'NN_i' 5: If ('NN_i' forward 'P_i' with contents unchanged) or ('NN_i do not drop) then 6: Forward 'P_i' to its 'NN_{i+1}' nodes 7: Else 8: Do not Forward 'P_i' to its 'NN_{i+1}' nodes 9: Remove 'NN_i' node from the network 10: End if 11: End for 12: End

Fig 4 Detection Manager Neighbor Node Relay Selection algorithm

As shown in the fig 4, the Detection Manager randomly obtains the incoming packets of its neighbors. It passively listens to the communication to and from each of its neighbor nodes by auditing the contents of the HELLO message. If the contents of the HELLO message include the existence of all neighboring nodes along with the broadcast information (as provided in Fig 2), then the packets are sent to all the neighboring nodes.

On the other hand, if the contents of the HELLO message include a node not present in the network, then the packet cannot be forwarded due to the non-existence of the node and therefore packet drop occurs. Therefore, the mobile node is presumed as the malicious node by the Detection Manager and therefore isolated from the network. Here, in the proposed technique, intrusion detection is performed by means of detecting packet drops and modifications by the neighboring nodes. The deviation from normal behavior of a neighbor node is used as an indicator to identify the presence of the malicious node and isolate it from the network.

Fig 5 shows the Packet Dropping-based Malicious Node Isolation strategy to identify the malicious node and isolate it from the network. In the figure, Node 'A' is the attacking node and Node 'P' is the target node. The attacker node 'A' instead of sending HELLO messages including '$\{P, Q, R, S\}$', it sends a fake HELLO message that contains '$\{P, Q, R, S, T\}$' that include three neighbor nodes '$\{Q, R, S\}$' and one non-existent node '$\{T\}$'. According to the protocol, the target node 'P' will select the attacking node 'A'. So the node 'A' is the malicious node which drops the packet as identified by the DM and is isolated from the network.

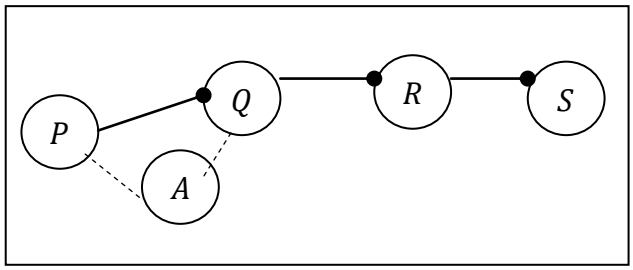

Fig 5 Packet Dropping-based Malicious Node Isolation strategy

In this way, a mechanism for detection of intrusion through packet dropping is presented based on cooperative nature of nodes in mobile ad hoc network. As a result, the faulty node that performs packet drop is identified as the malicious node and isolated from the network. This in turn ensures the security to a greater extent.

4. Simulation and performance comparison

To evaluate the proposed technique a real grid test bed simulator is required. However, to establish and maintain a real test bed is expensive. Instead, we choose a network simulator as the simulation tool. Many network simulators have been introduced, such as OPNET, NETSIM and NS2, among which NS2 is chosen since it provides a flexible and extensible simulation environment. In the following simulation, the existing intrusion detection techniques including Rateless Codes and Belief Propagation to Infer Identity of Polluters (RC-BP) [1], Enhanced Adaptive ACKnowledge (EAACK) [2] are implemented and compared with the IC-HCPD on a Mobile ad hoc network.

A random topology with a maximum of 70 nodes over a rectangle field was selected to test the proposed IC-HCPD and existing techniques RC-BP and EAACK respectively. The total dimension is fixed as 1500*1500m with the maximum transmission range of each mobile node being 250m and the duration of the simulation is 600s. Random way point model is used as the mobility model for each node.

The node speed is varied between 2m/s and 25m/s with the mobile node pause time is varied from 0 seconds to 300 seconds. In the result, for each metric, simulation is done for seven different seed values with taken for the result. Table 1 shows the parameters obtained that finally were used in the experiments.

Table 1 Parameters and values used in the experiment

Node density	10, 20, 30, 40, 50, 60, 70
Network area	1500*1500m
Transmission range	250m
Packets	9, 18, 27, 36, 45, 54, 63
Simulation period	600s
Minimum node speed	2m/s
Maximum node speed	25m/s
Node pause time	0 – 300 seconds

4.1 Simulation results

The tested algorithms were run on the same experimental environment as listed in table 1 so their performance can be fairly compared. Several test metrics were used. Routing overhead is obtained on the basis of the neighboring nodes in network. The mobile nodes in MANET often change their location within network due to the random changes in topology. As a result, some stale routes are generated in the routing table resulting in unnecessary routing overhead. A good algorithm is one which reduces the routing overhead. The routing overhead is formulated as given below.

$$RO = \sum_{i=1}^{n} NN_i * Time\ (NN_i) \quad (5)$$

From (Eq.5), the routing overhead 'RO' is obtained on the basis of the neighbor nodes 'NN_i' and the time taken to obtain the neighboring nodes '$Time\ (NN_i)$' in the network. Next, packet delivery ratio is used as the performance metric to measure the effectiveness of the proposed technique.

Packet delivery ratio is the ratio of number of packet actually delivered without duplication to destination verses the number of packet supposed to be received. This number or the packet delivery ratio represents the effectiveness and throughput of a protocol in delivering data to the intended receiver within the network.

$$PDR = \frac{P_d}{P_s} \quad (6)$$

From (Eq.6), the packet delivery ratio 'PDR' is measured using the packets delivered 'P_d' and the packets sent 'P_s' respectively. Finally, to evaluate the efficiency of the proposed technique, the rate of malicious behavior detection is measured.

Malicious behavior detection rate measures the rate of malicious nodes identified in the network. Due to different factors such as congestion, collision, packet drop, malicious behavior of a node is said to be observed. In the proposed technique, packet drop is used as a measure to detect intrusion in the network and is mathematically formulated as given below.

$$MBDR = \frac{Packet\ \ drops\ \ detected}{MN_i} \quad (7)$$

From (Eq.7), the malicious behavior detection rate '$MBDR$' is observed on the basis of the number of nodes or node density 'MN_i'. In the following, each simulation was performed seven times to obtain the values of the three performance metrics.

4.2 Routing overhead

A node density of 70 listed in table were employed to simulate the routing overhead using the three methods Integrated Cluster and Highest Connectivity-based Packet Dropping (IC-HCPD) Rateless Codes and Belief Propagation to Infer Identity of Polluters (RC-BP) [1], Enhanced Adaptive ACKnowledge (EAACK) [2] on mobile ad hoc network.

Table 2 Average node density and routing overhead

Node Density	Routing overhead (ms)		
	IC-HCPD	RC-BP	EAACK
10	0.38	0.45	0.60
20	0.52	0.59	0.64
30	0.78	0.85	1.09
40	0.95	1.03	1.18
50	1.05	1.12	1.26
60	1.15	1.22	1.35
70	1.28	1.35	1.50

A comparative analysis for routing overhead with respect to different mobile nodes was performed with the existing RC-BP [1] and EAACK [2] is listed in table. The increasing mobile nodes in the range of 10 to 70 are considered for experimental purpose in MANET.

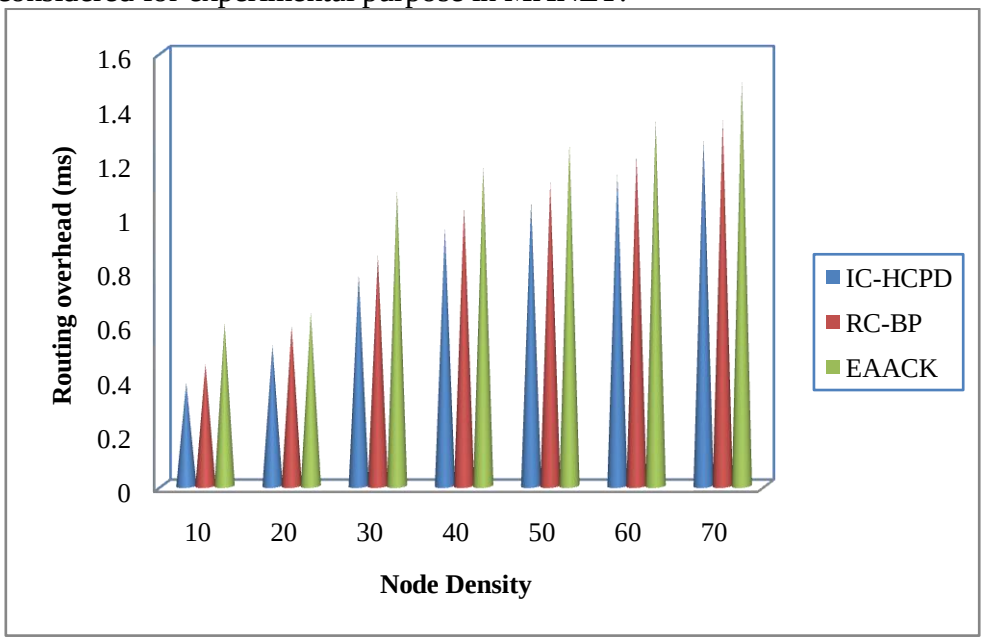

Fig 6 Routing overhead by varying the node density

Fig 6 shows the routing overhead for 70 nodes using the above mentioned intrusion detection techniques. As illustrated in fig, comparatively while considering more number of mobile nodes. In this simulation though three techniques have similar routing overhead, but were observed to be comparatively lesser when IC-HCPD was applied. The IC-HCPD method improves the routing overhead by considering neighbor node-based cluster formation that uses the minimum distance nodes for routing with respect to

different mobile nodes. The residual distance using the neighbor node information in IC-HCPD helps for any number of mobile nodes to obtain their neighbor information in a dynamic manner reducing the routing overhead by 9.64% compared to RC-BP and 28.50% compared to EAACK.

4.2 Packet Delivery Ratio

The experimental results in previous section have indicated that IC-HCPD method is more efficient than RC-BP and EAACK CR-DCST framework is more efficient than JSTM-EM and DIDS-WSN respectively in terms of routing overhead. In this section we compared IC-HCPD method with, RC-BP [1] and EAACK [2] to illustrate the effectiveness of applying clustering algorithm based on highest connectivity in terms of packet delivery ratio.

Table shows the performance of IC-HCPD, RC-BP and EAACK over different number of packets in terms of packet delivery ratio. From the table it is evident that the packet delivery ratio is observed to be high by applying the IC-HCPD method.

Table 3 Average packet delivery ratio and packets sent

Packets	Packet Delivery Ratio (%)		
	IC-HCPD	RC-BP	EAACK
9	92.35	82.45	80.32
18	94.19	84.24	81.12
27	95.23	85.28	82.16
36	89.21	79.26	76.14
45	91.35	81.40	78.28
54	93.28	83.33	80.21
63	95.89	85.94	82.82

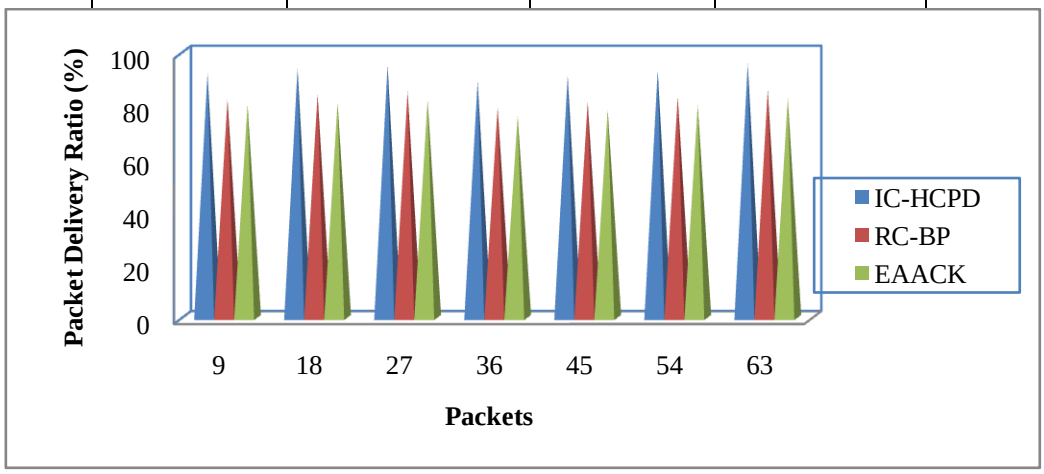

Fig 7 Packet delivery ratio by varying the packet density

Fig 7 displays the packet delivery ratio based on the changing number of packets. The mean packet delivery ratio of IC-HCPD method is improved by 11.15% and 1.46% compared to RC-BP and EAACK respectively. According to the highest connectivity as detected by the detection manager, the neighbor node that possesses maximum connectivity is selected as the route node through which the data or packets are forwarded. Therefore, with the highest connectivity, though existence of malicious nodes cannot be avoided, with the large number of neighbor nodes, the possibility of packet delivery ratio gets increased using the IC-

HCPD method when compared to RC-BP and EAACK. In case of the two existing methods, acknowledge information is used as a measure for data forwarding that ensures packet delivery. But the packet delivery ratio using IC-HCPD method was observed to be 10.68% improved and 1.39% improved when compared to the existing methods.

4.3 Malicious behavior detection rate

The malicious behavior detection rate using IC-HCPD method is provided in an elaborate manner in table with different number of mobile nodes and simulated using NS2 (as listed in table 4).

Table 4 Average malicious behavior detection rate

Node density	Malicious behavior detection rate (%)		
	IC-HCPD	RC-BP	EAACK
10	51.35	42.85	34.16
20	62.14	53.09	45.09
30	75.83	66.67	58.67
40	78.14	69.05	63.05
50	80.35	71.28	67.28
60	84.16	75.13	69.13
70	89.23	80.18	73.18

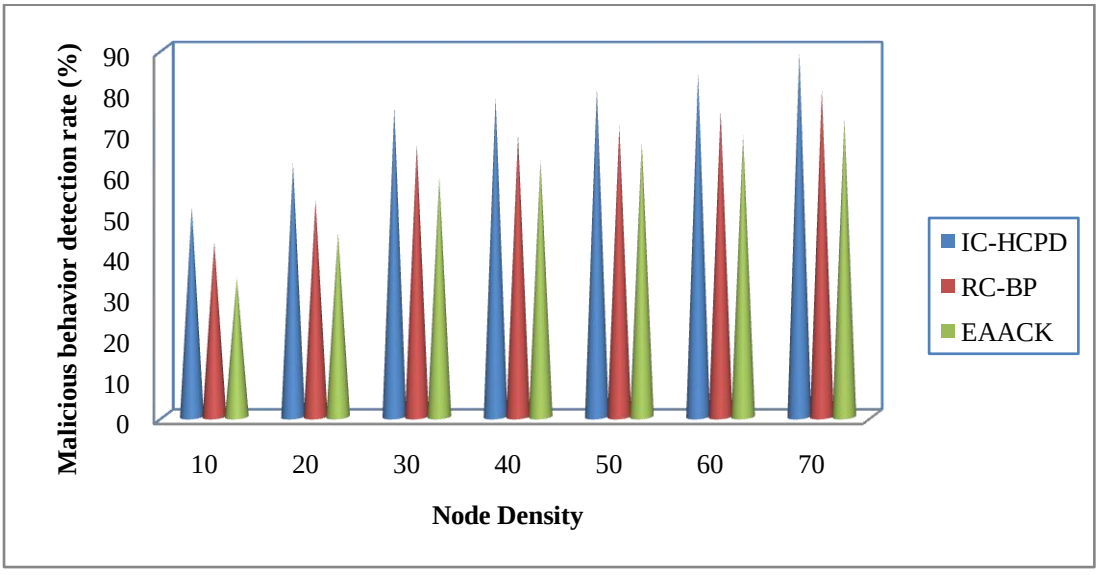

Fig 8 Measure of malicious behavior detection rate

Fig 8 shows the effect of malicious behavior detection rate for 70 mobile nodes. As node density increases, malicious behavior detection rate gets reduced. Here IC-HCPD outperforms the other methods as node density increases. The main reason is that the malicious behavior detection rate in the IC-HCPD method is made by isolating the malicious node based on the packet dropping rate. So the performance of the proposed Detection Manager Neighbor Node Relay Selection (DMNNRS) algorithm is improved by increasing the malicious behavior detection rate by 12.42% and 22.13% compared to RC-BP and EAACK.

5. Conclusion

Detecting intrusion in mobile ad hoc network is a complex task due to the intrinsic features of these networks, such as the higher node mobility, the lack of a fixed network infrastructure as well as the severe resource constraints. Therefore, there arises an urgent need to safeguard these communication networks and to propose efficient method in order to detect the intrusion at an early stage. In this article we provide an Integrated Cluster and Highest Connectivity-based Packet Dropping (IC-HCPD) that can be employed as intrusion detection method in MANETs. Results show that neighbor node selected based on the cluster formation may be a good paradigm to use when the goal is just to detect an intruder and isolate the intruding node from the network. The evaluation of the detection manager is performed considering highest connectivity that the intrusion detection process is completely distributed and maximum number of neighbor node exists in the network. Through the experiments using real traces, we observed that our intrusion detection method provided more accurate malicious behavior detection rate compared to the existing intrusion detection methods. In addition, our clustering algorithm based on highest connectivity effectively improved the packet delivery ratio and even reduced the routing overhead.

References

[1] Rossano Gaeta, Marco Grangetto and Riccardo Loti, "Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET", IEEE Transactions on Mobile Computing, Volume 13, Issue 7, July 2014, pp. 1482 – 1494.

[2] Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, March 2013, pp. 1089 – 1098.

[3] Peng Zhao, Xinyu Yang, Wei Yu and Xinwen Fu, "A Loose-Virtual-Clustering-Based Routing for Power Heterogeneous MANETs", IEEE Transactions on Vehicular Technology, Volume 62, Issue 5, June 2013, pp. 2290 – 2302.

[4] Yong Li, Pan Hui, Depeng Jin, Li Su and Lieguang Zeng, "Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices", IEEE Transactions on Mobile Computing, Volume 13, Issue 2, February 2014, pp. 377 – 391.

[5] Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb and Ali H. Afsaria, "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol", Elsevier, Procedia Computer Science, Volume 3, 2011, pp. 115 – 121.

[6] Dina Sadat Jalali and Alireza Shahrbanoonezhad, "A Novel Method Intrusion Detection Based on Sending and Checking Packet for Neighbored Nodes in MANET", Universal Journal of Communications and Network, Volume 2, Issue 1, 2014, pp. 10 – 13.

[7] Adnan Nadeem and Michael P. Howarth, "An Intrusion Detection & Adaptive Response Mechanism for MANETs", Elsevier, Ad Hoc Networks, Volume 13, 17 September 2013, pp. 1 – 28.

[8] Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila and Pedro Peris-Lopez, "Evaluation of classification algorithms for intrusion detection in MANETs", Elsevier, Knowledge-Based Systems, Volume 36, December 2012, pp. 1 – 9.

[9] S. Ganapathy, P. Yogesh and A. Kannan, "Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM", Hindawi Publishing Corporation, Computational Intelligence and Neuroscience, July 2012, pp. 10.

[10] Jaeun Choi, Gisung Kim and Sehun Kim, "A Congestion-Aware IDS Node Selection Method for Wireless Sensor Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, June 2012, pp. 6.

[11] Nabil Ali Alrajeh and J. Lloret, "Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, September 2013, pp. 6.

[12] Maha Abdelhaq, Raed Alsaqour and Shawkat Abdelhaq, "Securing Mobile Ad Hoc Networks Using Danger Theory-Based Artificial Immune Algorithm", PLOS One, 6 May 2015, pp. 1 – 16.

[13] Xuemei Sun, Bo Yan, Xinzhong Zhang and Chuitian Rong, "An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network", PLOS One, 8 October 2015, pp. 1 – 16.
[14] Wenchao Li, Ping Yi, Yue Wu, Li Pan and Jianhua Li, "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network", Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, June 2014, pp. 8.
[15] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Volume 9, Issue 8, August 2010, pp. 1119 – 1133.
[16] Kiran Mehta, Donggang Liu and Matthew Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", IEEE Transactions on Mobile Computing, Volume 11, Issue 2, February 2012, pp. 320 – 336.
[17] Shafiullah Khan, Kok-Keong Loo, and Zia Ud Din, "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks", The International Arab Journal of Information Technology, Volume 7, Issue 4, October 2010, pp. 435 – 440.
[18] Zubair Md. Fadlullah, Hiroki Nishiyama, Nei Kato and Mostafa M. Fouda, "An Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks", IEEE Network, Volume 27, Issue 3, June 2013, pp. 1 – 8.
[19] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks", IEEE Transactions on Mobile Computing, Volume 12, Issue 2, February 2013, pp. 1 – 15.
[20] Wei Gao, Guohong Cao, Tom La Porta and Jiawei Han, "On Exploiting Transient Social Contact Patterns for Data Forwarding in Delay-Tolerant Networks", IEEE Transactions on Mobile Computing, Volume 12, Issue 1, January 2013, pp. 151 – 165.