Journal of Scientific & Industrial Research
Vol. 79, October 2020, pp. 905-908

Reliability Integrated Intrusion Detection System for Isolating Black Hole Attack in MANET

S Gopinath[1]*, N A Natraj[3], D Bhanu[2] and N Sureshkumar[4]

[1]Department of Electronics and Communication Engineering, [2]Department of Information Technology, Karpagam Institute of Technology, Coimbatore 641 105, India

[3]Department of Electronics and Communication Engineering, Kathir College of Engineering, Coimbatore 641 062, India

[4]Department of ECE, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh

Received 4 March 2020; revised 12 May 2020; accepted 7 August 2020

Mobile ad hoc network (MANET) is a temporary network which can be utilized for emergency applications. It is easy to deploy the attackers in the network. The network performance may get degraded due to the presence of attackers. Black hole attack is the major attack which will totally violate the network rules and degrade the routing process. In this research, the Reliability Integrated Intrusion Detection System (RIIDS) is used for isolating the black hole attacks. It contains three phases. In first phase, the node forwarding ration is estimated to provide node reliability. In second phase, route reliability metric is evaluated to obtain the effective routes which can withstand the attackers. In third phase, objective function with effective routing strategy is adopted to detect attackers and isolate them by discovering alternate routes. The simulation results are analyzed using AODV protocol in terms of various performance metrics i.e. attacker detection ratio, queuing delay, packet delivery ratio and confidentiality.

Keywords: AODV, Node reliability, Packet delivery ratio, Queuing delay, RIIDS, Route reliability

Introduction

Mobile Ad hoc Networks and Impact of Black Hole Attack

Mobile ad hoc network is an infrastructure less network where nodes are connected and randomly located in the network. Black hole attack is one of the major attacks which discover the fake route and tunnel the data packets between source and destination node. Due to this attack, the packet dropping will be more which may lead to least packet delivery rate. The performance of network was analyzed in the presence of black hole attacks[1–5] and trust metric was computed to find the attack. Based on trust vector and link lifetime, the security level of path is identified and integrated with fuzzy mechanism. From the trust vector, the misbehaving nodes were found and isolated from the network easily. The concept of updating reputation table was introduced to prevent black hole attackers inside the network. In each route maintenance process, threshold vector value is maintained based on trust and energy levels. The reliability of routing was increased using message digest algorithm MD5 to secure data transmission between two nodes. The security challenges and goals of ad hoc networks were discussed to fight against attackers to provide reliable transmission and also to mitigate black hole attackers. The protocol used here was on demand vector routing protocol which supports routing for overhead reduction and minimization of delay. During dynamic environment, the fitness of node was estimated based on mobility, link lifetime and trust. Based on features and characteristics of intermediate node, the fitness value can be estimated to meet QoS standards. The intrusion detection system was developed and integrated to each route to provide authentication. The route discovery and packet forwarding process were discovered to improve the network performance during various dynamic scenarios. The trust management schemes were analysed to improve the route awareness to improve packet delivery ratio and reduce packet loss during route maintenance period. The trust threshold vector based key management scheme and ad hoc on demand vector routing protocol were combined together to provide authentication and improve network performance. Three factors were effectively calculated based on node competency, node integrity and relationship with the neighbor

*Author for Correspondence
E-mail: gopinath.ece@karpagamtech.ac.in

nodes. The concept of clustering and hybrid security mechanisms[6–12] were simulated using network reliable routing to avoid the black hole attackers but it was failed to reduce the attackers due to network density and lack of security deployment.

Experimental Details

Implementation of Intrusion Detection System

In this section, trust model is described based on node reliability metric, path trust and network topology discovery process. In the first calculation of node reliability metric, the packet forwarding ratio is estimated. It is assumed that each node can send 50 packets per traffic to neighbor node. The concept of collision avoidance scheme is used to identify the collision in the packets during data transmission. The packet forwarding ratio with respect to trust metric is estimated. The node reliability metric is used for the analysis of the secure path. For an example, the forwarding ratio $(R_{pq}(\tau))$ of node p and q is determined as follows,

$$R_{pq}(\tau) = \frac{NS_{pq}(\tau)}{NF_{pq}(\tau)} \quad \ldots(1)$$

The denominator ensures the number of packets forwarded successfully from source to sink node with loss and the numerator ensures the number of packets sent from source to sink node depends on the time period τ.

There are two groups constitute together to provide reliable transmission. The first group is request packets and the second group is estimation of packet forwarding ratio. Both are used to determine the node trust value.

Estimation of Route Reliability Process

In this phase, multicast route is established based on embedding reliable information in every packets. In general, multiple routes are discovered and they can compensate for dynamic environment but it is unpredictable to identify the attackers inside the network zone. In the proposed multipath route establishment phase, reliable information about paths is integrated in each and every packets moving towards the destination node. Here paths are considered as disjoint one. Nodes on disjoint paths are not unique. In this phase, cluster is formed and cluster head is chosen based on received signal strength and residual energy. Based on mesh based multicast routing, CH broadcasts the group of messages to multiple destinations via multiple paths. Once the CH received the joint reply packets from destination and intermediate nodes, multicast connection will be established based on link reliability and residual energy of nodes. The Multicast Route request packet contains source id, sink id, sequence number id (to check link activeness), link reliability, and residual energy. After receiving the route request packets from the source node, intermediate node checks the path reliability metric.

The routing path from source to sink node is determined according to node reliability based on forwarding ratio. There are two groups constitute together to provide reliable transmission. The first group is request packets and the second group is estimation of packet forwarding ratio. Both are used to determine the node trust value. The concatenation of reliability depends on propagation of node trust through reliable path. Each neighbor node assumes the nearby node is reliable and generic. It is ensured by the mechanism of reliability of packets and forwarding capability of nodes inside the network. The request packet is a crucial metric to determine the reliability of routes. The initial value of node reliability is set to zero. It is increased by 1 while forwarding packets to intermediate node in a short periodical time. The reliable value of path in each route discovery process for node p is determined as follows,

$$RR_{pq}(\tau) = R_{pq}(\tau) \times PR_p^{REQ} \quad \ldots(2)$$

The reliable value of path in each route discovery process for node q is determined as follows,

$$RR_{pq}(\tau) = R_{pq}(\tau) \times PR_q^{REQ} \quad \ldots(3)$$

The objective metric of trust enhanced on demand vector routing is determined based on route reliability and hop count during route maintenance process. There are three certain cases involved to determine the network reliability i.e. route reliability metric, hop count metric and route reliability metric and hop count metric alone.

Based on the trust case metrics x_1 and x_2, the objective function determines the quality of path during route maintenance phase.

Effective Routing Strategy for Detecting Black Hole Attack

The following steps are used to improve the routing performance.

Step 1: The source node looks up in its history table for the sink node before transmission.

Step 2: If any data presents in route history table, it initiates the data transmission through the nearby hop to sink node.

Step 3: If no routes found in the table, the route discovery process will be initiated to discover a new route to destination.

Step 4: Source node sends the data packet to sink node based on node reliability and route reliability metric.

Step 5: The intermediate node finds the absence of attacker pattern which is used to find the black hole or gray hole attacks.

Step 6: If any node goes below the value of trust threshold of node or packet reliability metric, it will be considered as misbehaving node and it will be immediately identified using intrusion detection scheme.

Step 7: The crypto scheme is adopted to provide encryption and decryption of data packets.

Result and Discussion

Performance Analysis

The proposed intrusion detection system is evaluated using Network simulator tool (NS 2.32). Totally 150 nodes are deployed for analytical purpose. Constant bit rate traffic is used and 250 meter transmission range is used. The simulation parameters are tabulated in Table 1.

Network Performance Metrics

Attacker Detection ratio: It is the ratio of finding attackers in the presence of all mobile nodes.

Packet delivery ratio: It is the number of packets received to the number of packet sent form source to sink node.

Confidentiality: It is the number of genuine packets travelling towards the sink node.

Queuing delay: It is the propagation of packet delay originated from source to sink node.

The results of packet delivery ratio while varying the numbers of reliable nodes in the route are given in Fig. 1. In existing schemes, the packet transmission begins through the random nodes only. In the proposed IDS, after the discovery of reliable routes and node, the packet delivery ratio is estimated and it is increased and produced high performance than exiting schemes.

Table 1 — Simulation and Setting Parameters of RIIDS

No. of Nodes	150
Area Size	1100 X 1100 sq.m
Mac	802.15.4
Radio Range	250 meter
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Walk
Protocol	AODV

The analysis of confidentiality is given in Fig. 2. The proposed scheme provides high rate than existing schemes. It is because of calculation of packet reliability before transmission.

In Fig. 3 the simulation results of attacker detection ratio are given. From the analysis, it is seen that detection ratio of proposed system is higher than existing schemes due to the adaptation of effective routing strategy.

In Fig. 4 the queuing delay is illustrated. In this analysis, the proposed system achieves less queuing

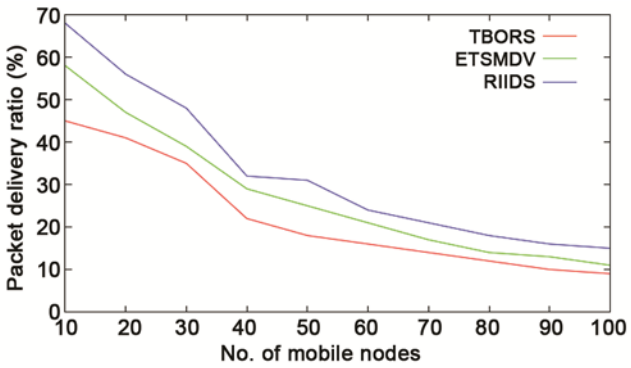

Fig.1 — Packet Delivery ratio Vs No. of Mobile Nodes

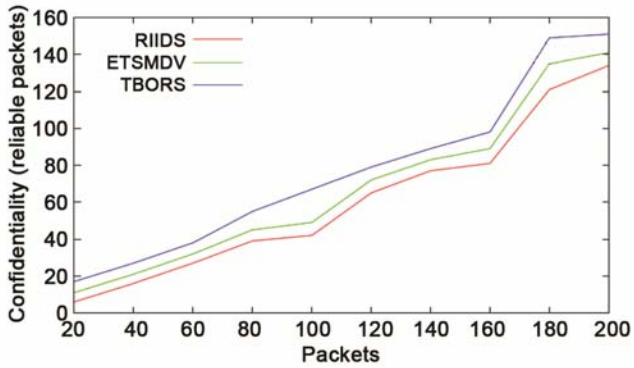

Fig. 2 — Confidentiality Vs Packets

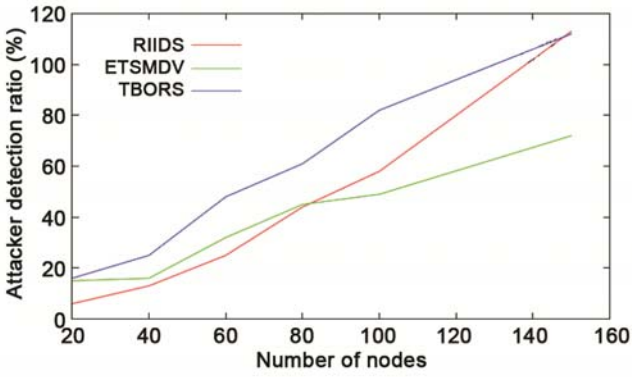

Fig. 3 — Attacker detection ratio Vs No. of Nodes

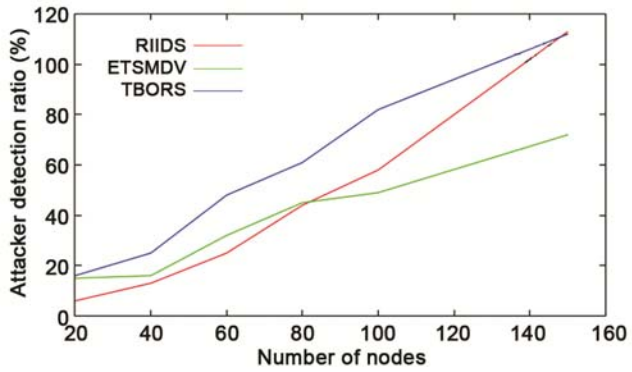

Fig. 4 — Queuing delay Vs Pause Time

delay than existing schemes due to the identification of reliable routes. If reliability persists, the delay of packet can be reduced effectively compared to existing schemes.

Conclusions

In MANET, it is easy to inject the attackers to degrade the performance of network. Due to the absence of access point, the node is compromised by the attackers. In this case, the detection and isolation of attackers is of high importance. In this research work, reliability enhanced intrusion detection system is used for isolating the black hole attacks in the network. Both packet and route reliability metric are calculated to isolate the misbehaving nodes in the network. The route strategy is found and installed before information transmission. The simulation results show the performance of proposed system which is comparatively higher than existing schemes.

References

1 Patel S S & Mohanpriya M, Trust based opportunistic routing scheme, *Int J Appl Eng Res*, **10** (2017) 2123–2126.

2 Sripriya G & Santha T, A secure trust based routing protocol for scheme enhancing quality of service in mobile AdHoc networks, *Int J Eng Tech*,**7** (2018) 717–722.

3 Gupta A & Dubey A, Advanced technique using trust based approach for prevention of black hole attack in mobile Ad Hoc network', *Int J Eng Appl Mang*, **2** (2018) 84–89.

4 Yasin A & Zant M A, Detecting and isolating black-hole attacks in MANET using timer based baited technique, *Wirel Commun Mob Comput*, **1** (2018) 1–11.

5 Shinh B, Novel technique to detect and isolate black hole attack in MANET, *Int J Eng & Comput Sci*, **6** (2014) 6513–6519.

6 Kaur V & Rani S, A hybrid and secure clustering technique for isolation of black hole attack in MANET, *Int J Adv Res Comput Sci*, **3** (2018) 230–237.

7 Khan S, Usmany F, Matiullahz & Khalil F K, Enhanced detection and elimination mechanism from cooperative black hole threats in MANETs, *Int J Adv Comput Sci Appl*, **3** (2018) 374–384.

8 Rao S V & Chauhan S, A hybrid and secure clustering technique for isolation of black hole attack in MANET, *Int J Rec Tech Eng*, **4** (2019) 491–495.

9 Thakur M, Gill A K, Detection and isolation technique for black hole attack in wireless sensor network, *Int J Adv Res Comp Sci Softw Eng*, **8** (2017) 25–29.

10 Bhalsagar S S, Chawhan M, Suryawanshi Y & Taksande V K, Performance evaluation of routing protocol under black hole attack in manet and suggested security enhancement mechanisms, *Int J Innov Tech Explor Eng*, **5** (2019) 1–7.

11 Singh M & Mandal J K, Reliability of MANET under the influence of black hole attack in adhoc on demand distance vector routing protocol, *J Sci Ind Res*, **76** (2017) 423–426.

12 Yadav R K & Mishra R, An authenticated enrolment scheme of nodes using blockchain and prevention of collaborative blackhole attack in WSN, *J Sci Ind Res*, **79** (2020) 824–828.