Detect and Prevent Active and Passive Attack in Autonomous Mobile Network

Sivasankar C\(^1\) and Kumanan T\(^2\)

\(^1\),\(^2\)Department of Computer Science and Engineering, Meenakshi Academy of Higher Education and Research Chennai, India.

\(^1\)Sivashankar.phd12@gmail.com

**Abstract.** In Autonomous Mobile Networks (AMNs), nodes regularly collaborate as well as transmit all packets to facilitate out of range transaction. Though, in unfriendly surroundings, several nodes might reject for preserve their own senders or for intentionally disrupting regular communications. In addition, the node mobility to handles the active and passive attacks. To overcome these problems, in this article Detect and Prevent Active and Passive Attack in Autonomous Mobile Network (DPAP) is introduced. Here, faithful forwarder node is chosen based on the vicinity information as well as connectivity of node. The active attacker node is detected by three hop verification method. In addition, the Binomial Pascal triangle function (BPTF) is applied for concealing the node uniqueness as a result; it recognizes the passive attack in the AMN. The DPAP approach is measured by applying a network simulator-2 for recognizing the active and passive attacker in the AMN. Simulation output illustrates the DPAP offer better throughput and detection ratio in the AMN.

**Keywords:** Autonomous mobile Networks, Three hop verification, Fibonacci Pascal triangle, Active and Passive attacker detection.

1. **Introduction**

Autonomous Mobile Networks (AMN) \(^1\) are endlessly, without infrastructure, self configuring created of a accumulation of mobile nodes lacking centralized direction. In this networks, every node can act a part as a node collaborating with other nodes \(^2\). As the main objective of routings to demonstrate aright as well as effective route by the disseminated nodes themselves also can communicate the data quick correctly. Besides the inactive attack in that the interlopers undertake to listen on the transaction, several types of active attacks incline to harm the AMN by altering the data that is more usual as well as destructive in AMNs.

A distinctive event is that the individual node malevolent otherwise the ordinate malevolent will compromise the AMN through directly attack otherwise indirect attack next leading the routing. In the direct attack, the malevolent can fiddle or loss the packets to construct the network paralytic, for example wormhole as well as the black hole attack \(^3\).

In indirect attack, the malevents advisedly update their own logarithms lacking determining the data communicating to disconcert the rectifying scheme. The capacity to detect this malevolent otherwise...
the nodes assailed by these breaking nodes is further important to a various set of management jobs for example executing network answer ability [4], distinguishing malevolent as well as malevolent nodes, and applying faith policies in disseminated systems [5]. Thus, security is the significant subjects for data transaction over AMN. In the previous methods, several security-raised assesses have been introduced to enhance the security of data transaction over AMN. Traditional methods on security raised data communications admits the intentions of cryptanalytics techniques as well as system structures also security- raised routing protocols [6]. Their general goals are frequently to overcome several menaces over the Internet, admitting listening, faking, session pirating, etc. Resisted to selective drop attack (RSDA) strategy to supply efficient security versus selective drop attack. It achieves dependability in routing within invalidating the connection with the most prominent weight as well as assaying the elliptic curve digital signature technique for checking the node authentication. RSDA protocol rejects selective drop attacks through precluding the nodes from acquiring overloaded. However, This strategy cannot prevent the data from the eavesdropper attacker [7]. To overcome this problem, In this paper we propose, Enhanced Audit-based malevolent Node revealing and secret Data Communication in Autonomous Mobile Network. Here, the Audit-based malevolent revealing (AMR) is introduced for discovering and separating malevolent nodes in AMNs. In AMR contains reputation phase, route discovery phase, audit phase. It constructs route comprising of greater faithful nodes. In addition, the Bivariate pascal triangle function (BPTF) is utilized for hide the node originality in the network.

2. Related work
A trust based security protocol that reaches authentication of data packets. In this scheme, every node keeping trust counter for observing and separating the malevolent node in the network [8]. However, this scheme cannot provide confidential data transmission in the network. Security of Cryptographically Generated Addresses using Adjustable Key [9] mechanism using AES algorithm. In this scheme, the every sub key is used to encrypt one AES block, using Mix-Column transformation in the original AES-128 to diminish the encryption time. In addition, the S-box and Inverse S-box are substituted by mere S-box utilized for encryption and decryption. However, this scheme does not provide node authentication in the network. Quorum time slot adaptive concentrating protocol [10] is introduced for attaining delay reduction and energy efficiency. the Quorum time slot is a packet communication period based on the features of data transmission that as a result extends the duty cycle of the nodes and diminishes the latency. Dij-Huff Method (DHM) is the compounding Dijkstra's and Huffman coding. Dijkstra's algorithm is utilized for discovering the nodes with best distance path and maximal energy and. Huffman coding is utilized for receiving security code. To offer security at every hop a individual security is being supplied known as Binary Hop Count [11]. Key distribution scheme adapt secure property by giving pairwise keys among nodes. Secure Connectivity scheme inquire the results of key distribution possibility on route length, queue size, and energy looseness while minimal cost routing is employed [12]. A key agreement scheme based on public discussion was described that attain a convinced secret key range while an opponent has more favourable situation. A secret key agreement protocol introduced the reliable relay regarded in the discourse to attain both reward distillation and secrecy elaboration [13]. Numerous key management approaches inserted to initiate symmetric keys [14]. This approach applying arbitrary seed dissemination with transient master key which offer pairwise keys. This approach approach discover the main disadvantage is providing less security. Masquerading Attack detection system (MADS) using the received signal-strength (RSS). In this method, the Signal strength variation is used to detect the attack accurately. The RSS is a lightweight cryptographic certification that as well does not necessitate extra charge to the present wireless technology. Although, the RSS is not quite authentic since it changes as well as fluctuates over time owing to several elements, for example multipath passing, deflection, etc [15]. Modified Russian Peasant Multiplier based on Divide as well as conquer method is utilized for multiplication procedure. Minimizing the chip size, enhancing the quickness as well as minimizing the energy depletion are key critical issues in System strategy [16]. An opportunistic routing by responsiveness of energy to accept by dynamic environment. While the sender transmits the information to a multicast group, the sender transmits the information via greater energy between vicinity thus enhance the life span [17].
3. Detect and Prevent Active and Passive Attack in Autonomous Mobile Network

This method faithful forwarder node is chosen based on the vicinity information as well as connectivity of node. It initiates throughout the reply of route packet communication explicitly a packet utilized to inform the sender which the route is detected. Here, the active attack is detect by three hop and passive attacks

3.1 Active Attack Detection

The figure 1 illustrates the three hop verification of nodes in the chosen route for communication. The receiver is the initiating point. It is executed among adjacent nodes.

![Figure 1. Three hop verification](image)

Primary it is employed among the receiver as well as mobile node A, next among node A and node B, then among node B and the sender. Adjacent nodes which should transmit frankly seek for a substitute minimum distance among them with an utmost length of three hops. The substitute least route is explored from vicinity lists. This scheme, the active attack detected by two phases of examination that is executed among adjacent nodes in the chosen route. Assume the transfer node in the chosen route is A as well as the receiver of A is B; B is the next node to A in the route. The two phases of examination are executes among node A and B. Winning the initial phase represents the mobile node is faithful then no necessitate to go by the next phase. The initial phase of examination is to construct an initial hop vicinity table for A as well as an initial hop vicinity table for B. Next, to verify if exist a common node among the two tables. If not present, it goes via the next phase of verification. In the next phase, A verifies whether exist is a three hops route to node B also B performance the identical. This process is done via the node A utilizing the one hop vicinity list it is established in the initial phase. When, B constructs its two hop vicinity list. B constructs it via calling for each node in its earlier one hop vicinity list to transmit their individual one hop Vicinity lists

3.2. Passive Attack Detection

Here, the Sender does not display actual identity of in-between, receiver and itself. Data communication routing nodes are reproducing of its BPTF values. The malicious node supervises the transaction although does not recognize Sender, in-between and receiver of the route. The BPTF task is determined as
Figure 2. Fake Route creation

\[ \text{BPTF} = (Q - R)^k \]  

(1)

Where, \( Q \) denotes the Source \( R \) denotes the destination as well as \( k \) represents the hop count of in between nodes.

The figure 2 demonstrates the fake route creation in AMN. Here, the node 6 is a Sender, 7 is a receiver also in between nodes are 9, 3. These nodes are makes a fake route through the BPTF.

\[
(6 - 7)^3 = 6^3 - 3(6)^2 (7) + 3(6)(7)^2 + (7)^3 \\
= 216 - 126 + 882 + 343
\]

From figure 2, the unique identity of the sender is 6 but, BPTF makes the fake identity is 216 also the receiver unique identity is 7 though fake identity is 343. Equally, the in between nodes 9, 3 maintains the fake identities are 126 and 216. This fake path creation creates additional competent as well as the passive attacker dos not identify the unique identity of the nodes. So, passive attacks are diminished throughout data communication.

4. Performance evaluation

To execute simulation examination, we utilized the NS-2.35 that incorporates the 802.11 MAC protocol. This protocol is functioning on the 2.4 GHz physical layer and each sensor node transaction range is preset to 180 metre. In this simulation topology, the BS node plays Owner of complete network as well as every sensor node function is sensing, data forwarding as well as obtaining the data. The packet traffic is yielded with constant bit rate. This simulation examination, we measured the following metrics namely Packet Obtained Rate, Latency, Packet Dropped Rate, Throughput and detection ratio.

4.1. Packet Obtained rate (POR)

It is defined as the ratio among the amount of data packets perfectly obtained by the receiver and the amount of data packets yielded by entire mobile nodes.
From this figure 3, the proposed method DPAP is greater compare to the existing method RSDA. Since, the DPAP pick the route by the consistency path. Thus, enhances the routing efficiency.

4.2. Packet Drop Rate (PDR) Analysis
It is denoted as the distinction among the forward packets and obtained packets in the communication MANET per particular time. PDR is measured by Equation 4.

\[ PDR = \frac{\sum_0^n \text{Forward Packets} - \text{Obtained Packets}}{\text{Time}} \]  

From this figure 3, the proposed method DPAP is greater compare to the existing method RSDA. Since, the DPAP pick the route by the consistency path. Thus, enhances the routing efficiency.

Figure 4 illustrates the PDR of RSDA as well as DPAP. It indicates the successful transaction between nodes in the AMN. From this figure, DPAP execute lesser PDR of the RSDA scheme. DPAP scheme observes the active and passive attacker nodes from the path; thus it dilutes the PDR in the AMN.
4.3. Latency
It is defined as the time period from while the data packet communication is initiated at the source to while the data packet is perfectly obtained by the sink.

\[
\text{Latency} = \frac{\sum_{n=0}^{n} (\text{Packet Obtained Time} - \text{Packet Forward Time})}{n}
\]  

(5)

\[\text{Throughput} = \frac{\sum_{n=0}^{n} \text{Packets Received}(n) \times \text{Packet size}}{\text{Time}}\]  

(6)

\[\text{Figure 5.} \quad \text{Latency of RSDA and DPAP}\]

The figure, 5 illustrates the latency of RSDA as well as DPAP. The data traverse via link consistency factor nodes. Thus minimizes the routing latency.

4.4. Throughput
It is the vital parameter for measuring the operations of network. In this protocol, the throughput is specified as the amount of data packets effectively obtained at the receiver.
Figure 6. Throughput of IEET and LCEE

The figure 6 proves the DPAP scheme has higher throughput. Because of, RSDA scheme concentrate only the energy efficiency. But, DPAP focuses the link consistency thus DPAP has provide better performance in AMNs.

4.5. Detection Ratio
Here, we observe the RSDA and DPAP routing protocol for detection ratio and false detection ratio. The detection ratio is determined as given below:

\[
Detection \ Ratio = \frac{Detected \ nodes}{Whole \ nodes}
\]  

(7)

\[
False \ Detection \ Ratio = \frac{Mistook \ attacker \ nodes}{Whole \ nodes}
\]  

(8)

Detection ratio represents the count of attacker nodes discovered through usual nodes. False detection ratio represents the number of usual nodes mistook as the attacker nodes through usual nodes.

Figure 7. Detection Ratio of RSDA and DPAP
The detection ratio of RSDA and DPAP protocols are projected in Figure 7. It illustrates that the detection rate of DPAP is better than RSDA protocol due to the FPTF as well as three hop verification methods are recognize the active and passive attacks in the AMN.

![Figure 8. False Detection Ratio of RSDA and DPAP](image)

Also the false positive ratio is diagrammed for the RSDA and DPAP schemes in Figure 8. It illustrates the DPAP has lesser false negative ratio than the RSDA scheme.

4.6. False Detection Ratio

Here, we observe the RSDA and DPAP routing protocol detection ratio. The detection ratio is determined as given below:

\[
\text{Detection Ratio} = \frac{\text{Detected nodes}}{\text{Whole nodes}}
\]  

5. Conclusion

AMN is an important domain in current years owing to rapid dissemination of wireless devices thus the safety is a vital effect. The three hop verification is employed for identifying active attack. The Fibonacci Pascal Triangle Function is applied for recognizing passive attack in the network. Fibonacci Pascal Triangle Function method makes the fake route to defend the data from the passive attacker. Consequently, the sender transmits data through the normal nodes and receiver gets the secret routing information throughout data communication. Simulation outcomes illustrate both the highest packet obtained rate and detection ratio and lesser delay in the AMN.

References

[1] Yu W and Liu KR 2007 Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks *IEEE Transactions on Mobile Computing* 6 507-521
[2] Shen WL, Chen CS, Lin KCJ and Hua KA 2012 Autonomous mobile mesh networks. *IEEE Transactions on Mobile Computing* 13 364-376
[3] Jain S and Khuteta A 2015 Detecting and overcoming blackhole attack in mobile Adhoc Network *Int. Conf. on Green Computing and Internet of Things (ICGCIoT)* 225-229
[4] Thamilarasu G and Ma Z 2015 Autonomous mobile agent based intrusion detection framework in wireless body area networks *16th Int. symp. on a world of wireless, mobile and multimedia networks (WoWMoM)* 1-3
[5] Chen CL, Chen SC, Chang CR and Lin CF 2014 Scalable and autonomous mobile device-centric cloud for secured D2D sharing Int. Workshop on Information Security Applications 177-189
[6] Caiti A, Calabro V, Dini G, Lo Duca A and Munafo A 2012 Secure cooperation of autonomous mobile sensors using an underwater acoustic network. Sensors 12 1967-1989
[7] Poongodi T, Khan MS, Patan R, Gandomi AH and Balusamy B 2019 Robust defense scheme against selective drop attack in wireless ad hoc networks IEEE access 7 18409-18419
[8] Rajaram A and Palaniswami S 2010 Detecting malicious node in MANET using trust based cross-layer security protocol Int. J Comput Science Information Technologies 2 130-137
[9] Patil KT and Patil ME 2014 Improve the Security of CGA using Adjustable Key Block Cipher based AES, to Prevent Attack on AES in IPV6 over MANET IEEE Global Conf. on Wireless Computing & Networking (GCWCN) 148-152
[10] Liu Y, Ota K, Zhang K, Ma M, Xiong N, Liu A and Long J 2018 QTSAC: An energy-efficient MAC protocol for delay minimization in wireless sensor networks IEEE Access 6 8273-8291
[11] Alghamdi TA 2018 Secure and energy efficient path optimization technique in wireless sensor networks using DH method IEEE Access 6 53576-53582
[12] Yildiz HU, Ciftler BS, Tavli B, Bicakci K and Incebacak D 2016 The impact of incomplete secure connectivity on the lifetime of wireless sensor networks IEEE Systems Journal 12 1042-1046
[13] Wang N, Zhang N and Gulliver TA 2013 Cooperative key agreement for wireless networking: Key rates and practical protocol design IEEE Transactions on Information Forensics and Security 9 272-284
[14] Hemanth Kumar and Ramesh GP 2020 Energy efficiency and Data packet security for wireless sensor networks using African Buffalo Optimization IJCA 13 944-954
[15] Abbas S, Faisal M, Rahman HU, Khan MZ and Merabti M 2018 Masquerading attacks detection in mobile ad hoc networks IEEE Access 6 55013-55025
[16] Keerthi Anand VD 2015 Power Efficient Multicast Opportunistic Routing Protocol (Pemor) To Optimize Lifetime of Manet. Int. Journal of MC Square Scientific Research 7 109-127
[17] Sendhilkumar NC 2017 Design and implementation of power efficient modified Russian peasant multiplier using ripple carry adder Int. Jour. of MC Square Scientific Research 9 154-165