Credential Rate based Black hole attack Detection in MANET

Rameshkumar S G¹ and Mohan G²

¹,² Department of Electrical Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, India.

¹rameshkumarsg17@gmail.com

Abstract. Mobile Ad-hoc Networks (MANETs) are growingly being distributed in protection-essential applications. Since their integral resource-restrained features, they are prostrate to several security attacks as well as a black hole attack is a category of which critically involves data gathering. To defeat that dispute, Credential based Black hole attack Detection in MANET (CRBD) is anticipated for MANETs. In this scheme, the vicinity account (VA) checks node cooperativeness among neighbourhood nodes as well as obtained data-packet account (ODA) checks the data packet forward rate. The black hole attacker has least both ODA as well as VA. In addition, the black hole attacker has highest outstanding energy compared to the neighbour nodes. These parameters isolate the black hole attacker nodes in the network. The simulation examination demonstrates that the least packet loss as well as network delay.

Keywords: Credential Rate, Black hole attack Detection, vicinity account, QoS account, obtained data-packet account, energy account, Mobile Ad-hoc Networks.

1. Introduction

With MANETs contains group of mobile nodes that vigorously swap data between themselves lacking the confidence on centralized management otherwise permanent base station. Self-preparing feature alters MANETs to be simply demonstrated in an extensive selection of dissimilar positions, for example, liberate, tragedy performances, and battle ground transactions. Though, node motion and self-preparing features of MANETs reason modify of topography in an unpredictable method. Generally, every node with imperfect communication range has to get help of its vicinity nodes for data communications. Therefore, the execution of MANETs mainly based on the consistent path between nodes [1]. Though, the entire routing approaches are intended with a presumption that all nodes are completely reliable and prepared to collaborate with all other. As a result, they are susceptible to path interruption attackers that are not mutual or violate the path principles. Usually, dynamic black hole attack, inactive black hole attack as well as gray-hole attack is simply initiate the MANET [2]. In dynamic black hole, the attackers forever maintain that they have the shortest route to the receiver still it do not have any appropriate path information. Also, this types of attack losses the sum of data packets soundlessly. In inactive black hole, the attacker assists communicating path messages but remove the entire communicating data packets [3]. In gray-hole attacks, instantly losing entire communicating data packets, gray-hole attackers might selectively transmit data packets that can exploit their own concerns. However, both black hole attackers as well as gray-hole attack will not insert fake data into system, therefore they go to inactive path

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

Published under licence by IOP Publishing Ltd
interference attackers. The stay of this work is prepared as follows. In Section 2, the related work is surveyed. The Credential Rate based Black hole attack Detection in MANET (CRBD) is anticipated for MANETs is depicted in Section 3. In Section 4, present performance analyses. At last, finish in Section 5.

2. Related work

The node duplication attack recognition scheme [4] uses Danger Theory for finding duplicate nodes in the network. It recognizes the affected region via discovering the unnatural behavior of the nodes. It contains two major security phases such as attack recognition as well as security control. These phases execute a multi-level recognition that is dependable to recognize, alleviate as well as defend the duplication nodes in the network. Energy awake trust scheme [5] is provide sufficient security as maintain overhead by utilizing a game theoretic technique. This technique is functional to the trust origin method to diminish the overhead. Although, this scheme enhances the overhead of routing in the network. Evolutionary self-cooperative trust (ESCT) approach which emulates person cognitive procedure as well as swears on trust-level data is used to avoid different routing interruption attacks. In ESCT, movable nodes will swap trust details and examine obtained trust details by their own cognitive opinion. Finally, every node energetically acquires its cognition to eliminate malevolent units. The major appealing attribute of ESCT is that they cannot cooperation the organism even if the interior attackers identify how the safety method forms [6]. Generally, Vampire attacks are not specific to any type of protocol, but rather rely on the properties of many popular classes of routing protocols. The Vampire attack that hard to notice as well as simple to take out malevolent insider forwarding only tractable messages. This method is assists to alleviate these cases of attacks, considering a validation idea scheme that obviously restrictions injure induced with Vampires through the packet transmitting period [7]. The Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) is planned for movable users giving position proofs for every other in disseminated scenery. STAMP assures the honesty and non-interchangeability of the position proofs as well as defends users secrecy. Semi-trusted guarantee ability is utilized to allocate cryptographic keys and protector users against complicity with a light-weight entropy-based trust assessment method [8]. The jamming and the black hole attack as well as Denial of service attacks, are coverage of multi-tier HWNs. Every tier contains normal nodes, jammers as well as black holes. Assuming that productive examination function that involves a least obtained signal quality threshold to be achieved, get precise terms and concert bounces on the communication range possibility of random multi-tier with combined black hole attacks as well as jamming that based on the ability of nodes to identify also evade relationship with malevolent nodes [9]. Cooperative bait detection scheme (CBDS) technique assists for discovering malevolent node by applying a reverse tracing strategy. In this strategy, neighboring node’s tackle plays a bait receiver that assists to obtain a path respond since bait malevolent nodes. To discover the location of the malevolent node employs reverse retracing plan as well as detected malevolent node are stored in a list identified as black hole list. Then, noticed to entire nodes to break forwarding with that node rest in the list. Thus avoid black hole nodes in the network [10]. Throughput is enhanced with data-aided valuation method by means of transmit choice, channel then transmit obligation [11]. Authentication enables a node to ensure the identity of peer node. Authentication is essentially assured that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key [12].

3. Credential Rate based Black hole attack Detection in MANET

A black hole malevolent mobile node disseminates short route replies thus it may be chosen as majority appropriate node to route traffic. However, it loss entire obtained packets. To overcome this problem, this paper Credential Rate based Black hole attack Detection in MANET. Every node observes the packet communicating activities for every it’s one hop neighbors via discovering process. Here, every node has same resources like, transmitting power, queue size, energy as well as interface. In this scheme, every node disseminates hello messages in its transmission range nodes periodically. It consists of transmitter ID as well as credential rate. This credential rate is computed based on the node Energy
account (EA), Obtained Data-Packet Account (OPA), QoS account as well as Vicinity Account (VA). Figure 1 describes the structure of CRBD Scheme.

Figure 1. Structure of CRBD Scheme

3.1. Energy Account
The energy account (EA<sub>p,q</sub>) represents the outstanding energy in a mobile node. This computation is given below.

\[ EA_{p,q} = Initial\ Energy_{p,q} - Current\ Energy_{p,q} \]  

If the node energy is above the average outstanding energy that node is a black hole attack node.

3.2. Obtained Data-Packet Account (ODA)
It denotes the rate of data packets obtained from the transmitter node in the network. The obtained data-packet account is evaluating amount of exactly communicated packets to the amount of packets to be obtained. This computation is given below.

\[ ODA_{p,q} = \frac{ODR_{p,q}}{CDR_{p,q}} \]  

CDR<sub>p,q</sub> Indicates the sum amount of data packets communicated by node p as well as ODR<sub>p,q</sub> indicates the sum amount of data packets obtained by node q. If the ODA<sub>p,q</sub> is greater than 0.5 that node is normal node otherwise that node is a black hole. This computation is given below.

3.3. Vicinity Account
It denotes the rate of cooperative as well as uncooperative rate among two nodes. That identifies node characters in the network. This computation is given below.

\[ VA_{p,q} = \begin{cases} PC_{p,q} = \frac{Coop_{p,q}}{Coop_{p,q} + UnCoop_{p,q} + 2} \\ PU_{p,q} = \frac{UnCoop_{p,q}}{Coop_{p,q} + UnCoop_{p,q} + 2} \end{cases} \]  

where \( PC_{p,q} \) denotes the possibility that mobile node p believes mobile node q will perform cooperatively during hello packet dissemination action, as well as \( PU_{p,q} \) represents the possibility that mobile node p
believes mobile node q will perform not cooperatively during hello packet dissemination action. \( \text{Coop}_{p,q} \) as well as \( \text{UnCoop}_{p,q} \) are the cooperative and uncooperative rates that mobile node p controls for mobile node q. If \( \text{PC}_{p,q} \) or \( \text{PU}_{p,q} \) is larger than the threshold \( \alpha \), that mobile node represents the normal or black hole attack node in the network.

3.4. QoS Account

Quality of Service (QoS) is utilized for evaluating the function of the network. In this strategy, the node Qos is computed based on expression (4).

\[
Qos_{p,q} = \frac{ODR_{p,q} - DDR_{p,q}}{ODR_{p,q} + DDR_{p,q}}
\]  

(4)

where

- \( ODR_{p,q} \) - indicates the sum amount of data packets obtained by node q
- \( DDR_{p,q} \) - indicates the sum amount of data packets dropped by node q

Next, the Credential Rate (CR) is computed through the expression (5) given below

\[
CR_{p,q} = \frac{ODA_{p,q} + VA_{p,q} + EA_{p,q} + Qos_{p,q}}{4}
\]  

(5)

If the CR is greater than the Threshold that mobile node is a normal node otherwise that node is deceitful node.

![Node: CR](image)

Every mobile node its credential rate (CR) is stored in a table. This rate is denoted by 0 to 1. Where, 0.5 above trust rate represents the normal node and below 0.5 trust rate represents the malevolent node in the network. The CRBD approach assists getting the CR and it is exemplified in the figure 2. Here, the source S which is gets the CR value about its necessitating transmitting data. The mobile node with the highest CR value is selected as the credential hop and data is communicated to that special node.
4. Performance evaluation

The complete estimation of CRBD is executed using network simulation (NS-2.35). The primary energy of mobile nodes occupied as 1 joule as well as the CR threshold is 0.5. This topography contains 50 mobile nodes distributed arbitrarily region of 700x700m${^2}$. Here, we using the traffic is constant bit rate as well as the node packet size is 512 bytes.

4.1. Packet Obtained Rate Packet Obtained Rate (POR) Analysis

POR is denoting as the number of packets received at receiver per particular time. POR is assessed by Equation 6.

$$ POR = \frac{\sum \text{Packets Obtained}}{\text{Time}} $$  

(6)

Where, n = Node count

![Figure 3. Packet Obtained Rate of CRBD and CBDS](image)

The POR of CRBD and CBDS are diagrammed in Figure 3. It illustrates that the proposed scheme CRBD has 27.86% better POR when compared to the existing strategy CBDS.

4.2. Packet Drop Rate (PDR) Analysis

PDR is denoted as the distinction among the forward packets and obtained packets in the communication MANET per particular time. PDR is measured by Equation 7.

$$ PDR = \frac{\sum \text{Forward Packets} - \text{Obtained Packets}}{\text{Time}} $$  

(7)
Figure 4 shows the PDR values obtained from the simulation analysis of CRBD and CBDS. It indicates that PDR of CRBD is higher by 12.89% when compared with CBDS.

4.3. Outstanding Energy (OE) Analysis
Amount of energy outstanding in a node at the present occurrence of period is called as OE. A determine of outstanding energy commits at which energy is enthusiastic by the MANET functions.

Figure 5 indicates OE of the MANET is enhanced for proposed scheme CRBD when compared with CBDS. Around 0.09 joule of energy is saved per node by using the CRBD protocol for routing.

4.4. Throughput Analysis
Throughput denotes to an entire number of packets successfully delivered across network per unit time. Throughput is obtained using Equation 8.
(8)

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

Figure 6. Throughput of CRBD and CBDS

Figure 6 indicate the outcomes for throughput execution of existing strategy CBDS and CBDS versus CBR traffic. It is mentioned that the CRBD approach has 27.87% highest throughput while equated to the existing strategy CBDS. CRBD executes the node ODA, VA as well as EA as a result detect malevolent node then communicate the data. But, the existing strategy CBDS offers independence to malevolent nodes to loss extra data packets thus diminishes the throughput.

4.5. Delay Analysis

Delay is represented as the time period difference among data sent and packets obtained. It is measured by Equation 9.

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

Figure 7. Delay of CRBD and CBAD
Figure 7 demonstrate the execution estimation for average delay for CBAD as well as existing strategy CBDS. It is mentioned that the CBAD approach has 32.64% less delay while equated to the existing strategy CBDS. In existing approach increases the malevolent nodes raise in the system, the delay further more rises owing to enhance the amount of system disconnections. The CBAD obtains better execution owing to it select the path is consistency.

5. Conclusion
In this paper we deliberate a prototype for black hole detection utilizing Credential Rate in MANET. In this strategy, the mobile node credential rate is computed based on the node Energy account, Obtained Data-Packet Account as well as Vicinity Account. The black hole node has lowest vicinity account rate as well as node cooperativeness rate also highest energy account rate. These parameters confirm the black hole nodes in the network. Then the source sends the notification message and discover the reliable route via credential rate based route selection in the network. The simulation examination depicts that the CRBD strategy offers highest throughput and outstanding energy when compared to the CBDS strategy.

References
[1] El Houssaini MA, Aaroud A, El Hore A and Ben-Othman J 2016 Detection of Jamming Attacks in Mobile Ad Hoc Networks Using Statistical Process Control Procedia Computer Science 83 26-33
[2] Sarma KJ, Sharma R and Das R 2014 A survey of black hole attack detection in manet Int. Conf. on Issues and Challenges in Intelligent Computing Techniques (ICICT) 202-205
[3] Shahabi, M G and Bakhtiarian M 2016 A modified algorithm to improve security and performance of AODV protocol against black hole attack Wireless Networks 22 1505-1511
[4] Shaukat HR, Hashim F and Sali A 2014. Danger theory based node replication attacks detection in mobile wireless sensor network IEEE Symp. on Computer Applications and Industrial Electronics (ISCAIE) 18-23
[5] Duan J, Gao D, Yang C, Foh CH and Chen HH 2014 An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications IEEE Internet of Things Journal 1 58-69
[6] Cai RJ, Li XJ and Chong PHJ 2018 An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs IEEE Transactions on Mobile Computing 18 42-55
[7] Vasserman EY and Hopper N 2011 Vampire attacks: Draining life from wireless ad hoc sensor networks IEEE transactions on mobile computing 12 318-332
[8] Reddy PLK, Reddy BRP and Krishna SR 2016 Spatial-Temporal Provenance Assurance with Mutual Proofs for Location Based Services IJCSEST 1-5
[9] Hemanth Kumar and Ramesh GP 2020 Energy efficiency and Data packet security for wireless sensor networks using African Buffalo Optimization IJCA 13 944-954
[10] Dumne PR and Manjaramkar A 2016 Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs 5th Int. Conf. on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) 486-490
[11] Santhakumar R 2017 Resource allocation in wireless networks by channel estimation and relay assignment using data-aided techniques Int. Journal of MC Square Scientific Research 9 40-47
[12] Lingeshwari S 2014 Provisioning of efficient authentication technique for implementing in large scale networks (PEAT) Int. Journal of MC Square Scientific Research 6 34-42