Reliability of MANET under the Influence of Black Hole Attack in Adhoc on Demand Distance Vector Routing Protocol

M Marjit Singh¹* and J K Mandal²

¹Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology, Nirjuli-791109, Arunachal Pradesh, India
²Department of Computer Science & Engineering, University of Kalyani, Nadia-741235, West Bengal, India

Received 17 August 2016; revised 29 February 2017; accepted 27 April 2017

Enormous usage of Mobile Ad hoc Network (MANET) on regular basis in communication has generated keen interests towards research on reliability and security characteristics of MANET in recent times. Tremendous amount of research work on security in MANET are accessible in the literature currently. However, minimal amount of research on reliability analysis of MANET under security attack is available in the literature. The reliability analysis of MANET under black hole attack running Ad hoc on demand distance vector (AODV) routing protocol is accorded in this paper. The influence of black hole attack on the reliability of MANET is analyzed using ns-2.35 simulation software. It is revealed from the simulation results that the reliability of MANET under single black hole attack is higher than the reliability of MANET under multiple black hole attack in AODV routing protocol.

Keywords: Mobile Ad-Hoc Network, Network Reliability, Black Hole attack, AODV Routing Protocol

Introduction

Mobile Ad-hoc Network (MANET)¹² is a collection of small electronic devices called nodes that are embedded with processing power and capable of communicating with each other over wireless links. Limitations of MANET includes limited energy source of nodes, scalability problems, absence of central control, security threats and vulnerabilities. The MANET deploys routing protocols to transmit packets for communication. The protocols employed for MANETs are at risk to various types of network attacks for instance the black hole attack, sinkhole attack, wormhole attack etc. This paper presents the influence of black hole attack on the reliability of MANET running AODV (Ad Hoc On-Demand Distance-Vector) routing protocol. The reliability of the MANET without black hole attack, with single and multiple black hole attacks are analyzed respectively in AODV routing protocol. The simulations are performed in ns-2.35 simulation software. Tremendous work on performance analysis of MANET³ based on parameters such as delay, throughput etc. are available in the literature. This paper will accommodate the existing research gap on MANET reliability analysis under security threats and impart better MANET services.

Network reliability

The use of reliability engineering methods in design and execution of systems such as the computer networks are essential as we need reliable services from them. The probability that a system will carry out its planned functions appropriately over a stated time interval under known conditions of environment is known as reliability. It is the potential of the system to execute its anticipated operation over a stated time interval under defined conditions of utilization, but quantified in terms of probability. Reliability is concerned with probability of success, expected performance, intended time period and environmental conditions of use. Its value lies in between 0 and 1. Basic concepts on reliability engineering and network reliability are given by M.L.Shooman⁴. The probability of successful working of a network over a given time interval under stated conditions of environment is defined as network reliability. It is presumed that the network works uninterruptedly since the start/restart of the network. Successful workings of the network suggest the number of nodes that can exchange information with each other. Network reliability is also defined as the probability

*Author for Correspondence
E-mail: marjitm@gmail.com
of successful exchange of data between two specified nodes of the network. It is the probability of sending data from source node to destination node successfully. One can find ample amount of discussion on network reliability in the literature. Reliability of MANET is important and ensuring its reliability requires research. The ability to analyze reliability of MANET is the basic requirement towards ensuring reliability of MANET. The reliability of MANET is more fragile than that of traditional infrastructure based networks due to the impact of its features on the network connectivity. Research on MANET reliability is in developing stage. Survey on MANET reliability analysis is given out by Singh and Mandal.

The required and satisfactory network services provided by MANET can be quantitatively assessed by network reliability measures. Computing the probability of successful communication amongst a set of nodes for a specified period of time is the typical network reliability problem.

**Overview of AODV routing protocol**
Routing directs how the message is successfully transmitted from source node to destination node. MANET routing protocols are grouped as proactive (global), reactive (on-demand) or hybrid. The routes/pathes to all the target nodes (destinations) are obtained at beginning and periodically maintained using route update process in proactive routing protocol. In reactive routing protocol, the routes/pathes are determined as needed by the source by means of a route discovery process. AODV is a reactive routing protocol. It does not use source routing and it is on-demand. A path is established when required to transmit data by the source node. Using destination sequence number, the latest route to the destination is selected by AODV protocol. Each and every node in AODV (Ad hoc on demand distance vector) protocol maintains a routing table that keeps the next hop information along with destination sequence numbers for a path to the destination. AODV uses three control messages namely Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) for route discovery and maintenance process. RREQ message contain source and destination IDs, source and destination sequence numbers, hop count, broadcast ID and time to live. Source ID and broadcast ID acts as the identifier for RREQ. The source node that wants to communicate with another node will transmit RREQ message. An in-between node that has a path to the destination node produces a RREP and transmits it to the source node. RREP contains source ID, destination ID, latest sequence number of destination node and hop count. Each mobile node monitors the link status to its neighboring nodes. Whenever a link is detected as down, the RERR message is generated by the node and link failure status is notified to remaining nodes of the network. A source node will generate a RREQ message if it wants to start communication with another node. This RREQ message will be propagated to other neighboring nodes. This is forwarded/sent to successive neighboring nodes. Whenever the destination node or an in-between (intermediate) node that has a route to the destination node is found, a RREP message is sent to the source node and a route/path is established between source and destination nodes and they start to communicate. If a link is broken in such manner that reaching destination node from the source or intermediate nodes is impossible, then a RERR message is sent to the source node notifying that there exists a route error.

**Black hole attack**
MANET has several advantages over wired networks. But it is more susceptible against security threats compared to the security threats that exist in wired networks. The security threats and challenges in MANET are the consequence of its characteristics such as shared and wireless medium, constantly changing network topology etc. The wireless communication channel is available to the authorized users of the network as well as to the malicious attackers. Hence, security of MANET should be robust by providing efficient mechanism to defend the network from unauthorized/malicious attackers. When an attacker gets access to the network, it can launch a number of security attacks such as the black hole attack and hamper the network performance to a significant level. It may even break the normal working of the entire network. In black hole attack, the evil node convinces the source nodes in the neighbourhood of having a fresh and shortest route to the target node through it. The source node transmits its data packet through this evil node. Hence the evil node is capable of attracting the packets towards it through false manner. When it gets the packet, it can either drop all the packets or drop the packets
Proposed methodology

The MANET reliability computation method developed by Singh, Baruah and Mandal is applied in the paper. The series of steps of the proposed methodology is given below.

i. Create MANET Scenarios in ns-2.35 simulation software i.e. MANETs having 20, 30, 40, 50, 60, 70, 80, 90, 100, 110 nodes running AODV Routing Protocol.

ii. Compute reliability of each MANET using logistic regression.

- Use the logistic function: \( y = \frac{1}{1 + e^{\alpha z}} \); \( -\infty < z < +\infty \)

- \( z = \alpha \beta x_i \); \( \alpha, \beta \) are unknown variables, \( x_i \) is known variable.

- Estimate \( \alpha \) and \( \beta \) using maximum likelihood estimation with the parameters: \( x_i \) (max speed), \( s_i \) (packets sent), \( p_i \) (packets received), \( s_i - p_i \) (packet dropped).

- Estimate \( \beta \) using the formula: \( \beta = \left( x^T w z \right)^{1/2} \), where \( w_i = \mu_i (s_i - \mu_i) / s_i - p_i \), \( z_i = \log\left( \frac{p_i + 1/2}{s_i - p_i + 1/2} \right) \), \( \mu_i = \logit^{-1}(\eta_i) \), \( \eta_i = \ln \left( \frac{p_i}{s_i - p_i} \right) \).

iii. Record the reliability of each MANET obtained in step 2.

iv. Enforce single black hole attack in each of the MANETs created in step 1.

v. Repeat step 2 to compute MANET reliability with single black hole attack.

vi. Record the reliability of each MANET with single black hole attack obtained in step 5.

vii. Enforce multiple black hole attack in each of the MANETs by introducing more black hole nodes.

viii. Repeat step 2 to compute the MANET reliability with multiple black hole attacks.

ix. Record the reliability of each MANET with multiple black hole attacks obtained in step 8.

x. Compare the MANET reliabilities obtained in steps 3, 6 and 9.

Implementation and analysis

ns-2.35 simulation tool is used for obtaining results and analysis that generates a trace file through which the number of packets sent, packets received and dropped packets using variable maximum speeds and pause times of 10 seconds. The “Random way point model” is the mobility model adopted. Constant bit rate (CBR) traffic model has been used. The packet size is 512 bytes. The maximum number of connections among traffic sources is same as the total number of nodes. The simulation is performed on different sets of node grouping of the network beginning with 20 numbers of nodes to 110 nodes with an addition of ten nodes. The nodes are deployed in a boundary of 4000 mx 300 m topology. Simulation is performed without black hole attack and with single and multiple black hole attacks. The number of black hole nodes for multiple black hole attack considered in the simulation was more than two. The simulation framework and constants are given in Table 1. The simulation results that show the reliabilities of obtained in step 2.

<table>
<thead>
<tr>
<th>Network space</th>
<th>4000mx300m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes</td>
<td>20, 30, 40, 50, 60, 70, 80, 90, 100, 110</td>
</tr>
<tr>
<td>Maximum speed</td>
<td>5, 10, 15, 20, 25 m/s</td>
</tr>
<tr>
<td>Pause time</td>
<td>10 seconds</td>
</tr>
<tr>
<td>MAC layer</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>Mobility</td>
<td>Random waypoint model</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Simulation run time</td>
<td>100 sec</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>Ad hoc On Demand Distance</td>
</tr>
</tbody>
</table>

Network type          | Single and multiple black hole attacks |
MANETs running AODV protocol without black hole attack, with single and multiple black hole attacks are shown in Table 2. The graphical representation of comparisons of reliability against number of nodes in MANETs without black hole attack, with single and multiple black hole attacks running AODV routing protocols are presented in Figure 1. It is seen from the simulation results and the plots that the reliability of MANET with multiple black hole attacks is lower than the reliability of MANET with single black hole attack. However, we see that the reliability increases as the number of nodes increases in all node groupings of the network. The reliability is likely to decrease if there is an increase in the number of black hole nodes in the network.

Conclusion

In this paper, reliability analysis of MANET with single and/or multiple black hole attacks running AODV routing protocol is presented. It is seen from the simulation results that the reliability of MANETs with single black hole attack is higher than the reliability of MANETs with multiple black hole attack. The paper also presents the comparisons of reliabilities of MANETs without black hole attack, with single and multiple black hole attacks. As stated, huge amount of research on MANET are available but scanty amount of research work on reliability analysis of MANET under security attack is available. We will further investigate in this area covering other network attacks as well.

Acknowledgements

The authors acknowledge the support provided by the DST PURSE Scheme at University of Kalyani, and Department of Computer Science and Engineering, University of Kalyani, Kalyani, as well as North Eastern Regional Institute of Science & Technology (NERIST), Arunachal Pradesh.

References