Detection and Avoidance of Black Hole Nodes in MANETs
Zumer Jan¹, Nidhi Sharma²
Department of Computer Science Engineering
Swami Devi Dyal Institute of Engineering and Technology, Golpura, Barwala, Panchkula, India

Abstract:
In recent year with the widespread use of mobile device, Mobile Ad hoc networks (MANETs) technology has been attracted attention day by day. Since the MANETs don’t need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, MANETs in addition are used in personal area networks, home area networks and so on. Specially, MANETs suit for military operations and the emergency disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamic network topology of MANETs, infrastructure-less property and lack of certificate authority make the security problems of MANETs which need to pay more attention. The common routing protocols in MANETs such as DSR, AODV and so on almost take account in performance. They don’t have the related mechanism about detection and response. The information about the black hole node is broadcasted to the other nodes of the network to eliminate the uses of false route declaration. The BDSR detects and avoids the black hole attack based on merging proactive and reactive defense architecture in MANET by using the virtual and non-existent destination address to bait the malicious node to reply RREP. Finally the detected black hole node is listed in the black hole list and notices all other nodes in the network to stop any communication with them. As a result we can reduce packets loss that cause by the malicious nodes and have better packet delivery ratio.

Keywords: MANET, RA EED, AODV, Route Request, Route Reply, Route Error

I. INTRODUCTION
Mobile ad-hoc network (MANET) is referred as a temporary collection of heterogeneous and/or homogeneous collection of nodes (e.g. Source node, Destination node and intermediate nodes) targeting peer to peer data transmission. Each node is designed to behave like a router. Privacy and protection of data in ad-hoc network has been considered as a challenging aspect since the dawn of mobility. Black hole node problem is found as one of the major security concern nowadays. Detection and ignorance of black hole nodes leads to ensure a secure data transmission [1]. Each node among the MANETs not only works as a host but also need to play the role of router. While receiving data, nodes also need to help other nodes to forward packets, thereby forming a wireless local area network. However, the security of this particular network environment has many defects. In addition to the drawback of using radio wave to transmit in nature, there are still many problems, such as limited power, lower computing ability, and dynamic topology and so on. These problems make the security of MANET lower than cable network and produce many security issues [7]. Wireless Sensor Networks (WSNs) are composed of low cost, low power, small computing nodes, communicating wirelessly to monitor or control some aspect of the environment in which they are deployed. The main aim in WSNs is to route data from the nodes which detect some event in the environment (source) to the nodes requiring information about that event (sink or base station). Due to their broadcast transmission, unattended nature and hostile environmental conditions, there are many challenges to ensure a secure and reliable operation of a wireless network. In addition, the limited resources make the process more challenging in WSNs [4]. Mobile wireless communications have widespread use and applications in situation where we need to construct a quick temporary infrastructure less network, such as military services in battlefield, disaster relief and emergency operation, medical support, campus informal meeting etc [2]. Multiple concurrent node models are used in the formal framework because WSN comprised of more than one node. The node can be a source, a target, the destination or relay (intermediate) depending upon the particular routing protocol requirements. The base station (BS) or sink is also a node. However, in order to save the state space, the framework models it separately from the node model. The reason for this is that the sink model does not employ a complex functionality as required in the nodes and some details can be removed at the modeling stage. When an N node network is employed with one BS, there are N-1 node models and one sink model.

II. LITERATURE REVIEWS
Rajib Ghosh et.al in [1] introduced approach to detect and avoid black hole nodes during formation of reliable path for wireless data transmission. A valid acknowledgement is transmitted to the data packet sending node and its predecessor connected node. A trusted routing table created with valid acknowledgement receiver node. Secure data transmission is dependent upon the trusted routing table. Black hole nodes are required to be discarded from the data transmission. The information about the black hole node is broadcasted to the other nodes of the network to eliminate the uses of false route declaration.

Hizbullah Khattak et.al in [2] proposed scheme, used for the second optimal route for data packets transmission and hash
function for black and gray holes attacks avoidance and data integrity.

Junhai Luo et.al in [3] proposed for black hole prevention on top of Ad-hoc On-demand Distance Vector (AODV). The simulation results show the scheme provides fast message verification identifies black hole and discovers the safe routing avoiding the black hole attack.

Kashif Saghar et.al in [4] proposed a new protocol, RAEEED (Robust formally Analyzed protocol for wireless sensor networks Deployment), which is able to address the problem of black hole attacks. Using formal modeling we prove that RAEEED avoids this type of attack. Finally computer simulations were carried out to support our findings.

R Jaiswal et.al in [5] proposed a mechanism to mitigate single black hole attack as well as cooperative black hole attack to discover a safe route to the destination by avoiding attacks. In this paper we proposed an approach for better analysis and improve security of AODV, which is one of the popular routing protocols for MANET. Our scheme is based on AODV protocol which is improved by deploying Advanced DRI table with additional check bit. The Simulation on NS2 is carried out and the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection and elimination of the attack and maximizing network performance by reducing the packet dropping ratio in network.

Ume-Hani Syed et.al in [6] proposed to avoid Black hole attack in AODV. Proposed solution uses a route legitimacy value attached with RREP which ensures that the route is free from black hole node.

Po-Chun TSOU et.al in [7] proposed a DSR based secure routing protocol in this paper, named BDSR (Baited Black-hole DSR). The BDSR detects and avoids the black hole attack based on merging proactive and reactive defense architecture in MANET by using the virtual and non-existent destination address to bait the malicious node to reply RREP.

III. APPLICATION OF FORMAL MODELING TO DETECT BLACK HOLE ATTACKS IN WIRELESS SENSOR NETWORK ROUTING PROTOCOLS

A routing protocol is converted into a formal model (we call it Formal framework) and specification properties defined to check the presence of any fault (vulnerability to attacks) present in the routing protocol. The properties included basic sanity checks (confirmation that the model possesses some fundamental properties, debugging checks, etc.), the live-ness (something good will eventually occur) and the safety (nothing bad ever occurs). In case a property fails, the formal model checker automatically generates a trace providing the reason as to how the attack occurred in the protocol. The results are then confirmed and quantified using computer simulations. The formal framework comprises 5 main parts: attacker model, sink model, channel model, event generator (EG) model and node models. The protocol is checked against different DoS attacks independently, thus the attacker model is replaced for each specific attack. A black hole is modeled simply by modifying the node model which forwards all messages correctly except data messages. The channel model represents the topology and the capacity for communication between both legitimate (including BS) and malicious nodes. In UPPAAL, node connectivity (RF links) is modelled using an NxN topology matrix with 1 or 0 in matrix indicate existence or absence of an RF link, where N is the total number of nodes in the network. The node model contains a number of states depending on the protocol’s specifications. Each particular message passed between nodes in a protocol enables at least 2 states in the node model; ‘send’ and ‘receive’. Sometimes, more than 2 states are needed, e.g. before sending the data from the source node a ‘sense’ state models sensing data from environment. Apart from these states there is always a state in which a node does nothing and remains idle (listen state). Some other states in the node model are the ‘finish’ and ‘initial’ states, indicating the starting and the terminating states of a protocol. A subset of node model developed for RAEEED (Robust formally Analyzed protocol for wireless sensor networks Deployment), is shown in Figure Below.

Rajiv Kukreja - IJESC 2016 - Page 2565

**Figure: 1. Node Model (Data Forwarding Phase)**

IV.A NOVEL APPROACH FOR DETECTION AND AVOIDANCE OF BLACK HOLE NODES IN WIRELESS DATA TRANSMISSION

Routing methodology is one of the most important operations in a MANET. Any penetration in the routing technique causes direct impact on the whole network system. Routing is targeted by several external attacks. Dynamic, self-starting, multi-hop routing between mobile nodes are established and maintained in an ad hoc network. It has been empowered by Ad hoc On-Demand Distance Vector (AODV) routing protocol. In AODV, constructed route are not retained by the participated nodes. “Count to infinity” problem is avoided by the use of destination sequence numbers by AODV, a loop-free approach. Three types of messages are found in AODV:

i. Route Request (RREQ): used to initiate the route finding process

ii. Route Reply (RREP): used to finalize the routes.

iii. Route Error (RERR): used to notify the network about the link breakage.
AODV protocol has been used in between two unknown hops. A routing list contains IP addresses of neighbors are retained by each node. Routing table information must be kept for all routes. The routing table fields used by AODV are as follows: Destination IP Address, Destination Sequence Number, Destination Sequence Number Flag, Other state and routing flags, List of Precursors, Lifetime, Hop Count, and Next Hop information. The black hole attack is one of the important security threats in wireless AODV followed MANET. Black hole node problem affected the routing protocol by malicious node’s wrong RREP distribution. Shortest path advertisement to the destination node is claimed by the black hole node. The data packets are dropped during the data transmission through the advertised shortest routes.

![Figure: 2. Black Hole Problem](image)

V. CONCLUSION

The modeling and analysis of newly developed routing protocol RAEED was very helpful in detecting and preventing the black hole. The main emphasis was its vulnerability against black hole attacks after node compromission or via virtual links (wormhole and INA) between nodes. We have also performed computer simulations using TOSSIM on RAEED and compare the results with another secure protocol INSENS. The results confirmed that RAEED is more robust than INSENS. The detection and avoidance of black hole node during data transmission has been achieved in linear time. The packet delivery ratio has also been improved in the proposed methodology. The transmission has been stopped only when no other alternative true path remains.

VI. REFERENCES


