International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Spotting and Segregation of Sinkhole Node in MANET

Jeeja Borkar[1], Vaishali Malekar[2]

[1]RTMNU University, Kavikulguru Institute of Technology and Science, Maharashtra, Dt. Nagpur, 441106, Ramtek

[2]Kavikulguru Institute of Technology and Science, RTMNU University, Maharashtra, Dt. Nagpur, 441106, Ramtek

Abstract: ***MANET (Mobile ad-hoc Network) is mostly known for providing communication between nomadic nodes along with the different features such as, routing of data packets, managing whole network by self organization capabilities, interaction among nodes by maintaining trust factors. In MANET it is difficult to maintain the trust for nodes in the network. The different nodes communicate with each other by cooperating among the network. Due to these features MANET is more vulnerable to the different attacks. In this paper one of the attack detection and isolation mechanisms have been proposed. The point of concentration is to detect sinkhole attack. Presence of sinkhole attack will try to divert the whole network traffic towards itself or any other node by propagating wrong routing information in the network. In this paper the DSR (Dynamic Source Routing) algorithm is used for routing of data. Due to presence of sinkhole attack delay increases, network throughput decreases and packet delivery ratio decreases (PDR) and finally complete network leads to dead stage. This paper proposes the efficient method to deal with the sinkhole attack and make the network more efficient.***

Keywords: MANET, DSR, PDR, sinkhole attack, throughput.

1. Introduction

A mobile ad hoc network is a collection of wireless devices which can dynamically be set up without using any pre-existing infrastructure or central controller. In a MANET, nodes within each other's transmission range can communicate directly, whereas nodes outside each other's transmission range rely on other nodes to relay messages. Hence, a multi-hop scenario is created where every node functions as a router. The key features of MANET are autonomous terminals, dynamic configuration, distributed control, low profile terminals, bandwidth-constrained and limited physical security. MANET includes nodes and each node is an autonomous terminal, which functions as both a host and router. In other words, besides having the basic processing abilities of a host, the nodes in a MANET can also perform switching functionalities as routers. Then the endpoints and switches are indistinguishable in MANET. The participating nodes may join or leave the network without any disruption to users, the topology in a MANET may alter rapidly and unpredictably. In addition, the network may consist of both bidirectional and unidirectional links. And also there is no fixed infrastructure or central controller. The control and management of the network is distributed among the participating nodes and all the nodes in a MANET cooperate with each other and each node acts as relay as needed to security and routing. The mobile nodes have limited processing ability, small physical memory and limited power storage. Therefor the devices require optimized algorithms and energy conservation [7].

The wireless communication technology has been deployed in military since 1970s. This allows the military to maintain an information network between the soldiers, vehicles, and military information headquarters. Besides military communication, MANETs can also be deployed in scenarios where the pre-existing infrastructure has been damaged due to natural calamities (e.g., earthquake, tsunami, bushfire etc.), or human interventions (e.g., terror attack, theft etc.).

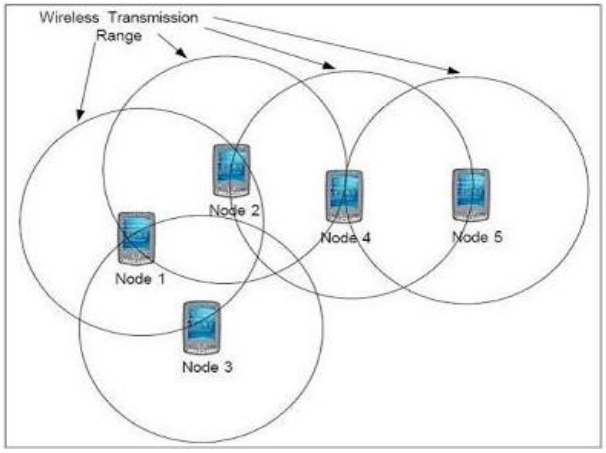

Figure 1: (a) MANET

Another application of MANET would be in the mining industry, where the workers deep underneath the ground level would be able to communicate with the base station. In addition, MANETs are also suitable to be used in a university campus, where the participants in seminar, or students performing an experiment at different corners would be able to share each other's views. In general, ad hoc networks can be deployed anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use [7]. Due to the lack of infrastructure and animatedly changing topology, the functionality of mobile wireless networks is highly reliant on the association of all nodes in the networks. In early days MANET was designed for military applications, but, nowadays it has used for new practice such as search and rescue operation, data gathering, virtual classes and conferences where laptops, palmtop, tablets or other mobile devices are in wireless communication [5].

Routing in MANET basically involves two activities such as determining optimal routing paths and transporting information groups (typically called packets) through an

internetwork. Routing algorithms have a distinct impact on network and router resources and they uses a variety of metrics that affect the calculation of best possible routes. The DSR and AODV are reactive routing protocols in ad hoc networks [1].

DSR Dynamic Source Routing (DSR) uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet. This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms Route Discovery and Route Maintenance. Route Discovery is used when the sender does not know the path up to the destination. In this mechanism, the sender broadcasts a ROUTE REQUEST message which contains Source Address, Destination Address, and Identifier. Each intermediate node adds its address in ROUTE REQUEST message and rebroadcast it, unless it has not rebroadcasted earlier. With this controlled broadcast, the ROUTE REQUEST will ultimately reaches the destination. The destination then sends a unicast ROUTE REPLY message in reverse direction whose information is obtained from list of intermediate nodes in ROUTE REQUEST message. When the ROUTE REPLY packet reaches the source, it records the route contained in it and saves in its cache for the specific destination. For better performance, intermediate nodes also records this route information from the two route messages. All nodes overhearing these packet add meaningful route entries in their caches. Finally, Route Maintenance Mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidates a cached route.

AODV Ad hoc on demand Distance Vector routing (AODV) is another on-demand protocol. It has similar mechanism of ROUTE REQUEST and ROUTE REPLY as that in DSR. However, it does not rely on source routing; rather it makes use of routing tables at intermediate nodes. The nodes maintain routing table entries of all reachable nodes in the network. The entries in routing tables are of the form: < Destination, Next Hop, No. of hops, Sequence Number>. Sequence number is used to maintain freshness. The route table is used to route data packets destined for a particular node and to respond to ROUTE REQUEST. The advantage of AODV over DSR is that, a data packet does not need to contain whole route to the destination.

2. Aim

The main aim is to detect and isolate the sinkhole node in mobile ad hoc networks, by substitution of routing protocol to enhance network capability after grievous attack. However, the open shared wireless medium and dynamic nature of MANET makes their routing protocols vulnerable to attacks for that the analysis of the on demand routing protocol is performed and also implement them to overcome the packet loss and energy consumption of nodes in mobile ad hoc networks.

Objective

- Detect misbehaving node in network
- To study the effect of sinkhole attack on network performance
- Isolate the sinkhole node from network
- Analysis of sinkhole attack behavior

3. Related Work

[1] Priya Malhotra, "Detecting Packet-Dropping Faults in Mobile Ad-Hoc Wireless Networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, pp. 558-561, February 2015.

Priya Malhotra [2] have proposed a method to deal with the network susceptible to Byzantyne faults with packets getting misrouted, corrupted or dropped. In this paper solutions have proposed using an unobtrusive monitoring technique using the Detection Manager to locate malicious or faulty nodes that misroute, corrupt or drop packets. The unobtrusive monitoring technique is similar to an intrusion detection system that monitors system activity logs to determine if the system is under attack.

[2] Sabarish D, Ranjani C, "Enhanced DSR Protocol for Detection and Exclusion of Selective Black Hole Attack in MANET", International Journal of Computer Applications, vol. 112, pp. 32-35, February 2015.

Sabarish D [3] et al [3] have suggested the Secure Dynamic Source Routing Protocol (SDSR) used to detect and prevent selective black hole attack. Selective black hole attack is a special kind of black hole attack where malicious nodes drop the data packets selectively. An Intrusion Detection System (IDS) have been proposed in this paper where the IDS nodes are set in promiscuous mode only when required, to detect the abnormal difference in the number of data packets being forwarded by a node.

[3] Nidhi N. Desai, Hiteishi Diwanji, J. S. Shah, "A Temporal Packet Marking Detection Scheme against MIRA Attack in MANET", IEEE Transaction, pp. 978-982, March 2014

Nidhi N. Desai [4] et al [4] has proposed a detection scheme to detect the malicious nodes at route discovery as well as at packet transmissions. This paper proposed detection scheme against MIRA attack in MANET. Misleading routing attack (MIRA) in MANET intend to delay packet to its fullest in order to generate time outs at the source as packets will not reach in time. Its main objective is to generate delay and increase network overhead. Proposed approach provides detection scheme at route discovery as well as at packet transmission.

[4] Sunil Phulre, Pratima Gautam, Sadhna K. Mishra, "Implementation of Trusted Multitier method for Intrusion Detection in Mobile ad Hoc Networks with DSR Algorithm", Science and Information Conference London UK, pp. 666-673, August 2014.

Sunil Phulre [5] et al [5] have propoed muiltier intrusion detection system. Here three tiers are application, routing and trust. First a trusted connection is established between different nodes. Second the routing policy is conformed for all nodes. Finally at the application layer data is routed on the type of application. The node which is not following trust or routing policy is considered a malicious node. In this paper different types of attacks have been simulated.

[5] Mohammed Ashfaq Hussain, A. Francis Saviour Devaraj, "Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET", International Journal of Engineering Research and Applications, vol. 3, pp. 1737-1741, April 2013.

Mohammed Ashfaq Hussain [6] have suggested that the presence of a sinkhole node on the network will affect the performance of the DSR routing protocol, with the help of parameters like network throughput, packet drop and packet delivery ratio. And the author have analyzed that a Sinkhole node will degrade the network performance to a large extent and hence must be detected and avoided.

4. Existing system

In the existing system different simulation parameters have been observed. The different network parameters like throughput, packet drop and packet delivery ratio are observed with the presence of sinkhole nodes on MANET and these results are compared with the absences of sinkhole node in the network. And along with this the each node have assigned with the different priorities which can take part in routing process based on the priorities assigned.
The above method is quite time consuming and this method does not give the efficient way to detect malicious behavior of the node.

5. Proposed system

5.1 Detecting Presence of Sinkhole Node on MANET

For detecting the malicious node, a detecting node sends a probe message to all nodes on a given path. When a node receives this message, send back an acknowledgment message to the sender. Therefore, if the sender dos not receive the acknowledgement from a given node, it assumes that the node is a malicious node.

5.2 Detect Actual Occurrence of Sinkhole node in MANET

Detecting node is the node that is aware of the existence of a sinkhole node in the network. This node initiates the detection phase. Our approach uses far to near probing, that's why detecting node sends a probe message to the last node on the sinkhole route, if it does not receive the acknowledgment from the given node, it will send the probe to the next hop. It repeats this until it receives an acknowledgment. Hence, it suspects to the previous node.

5.3 Isolation of Sinkhole Node in MANET

To prevent a sinkhole node to participate in route discovery, detecting node generates a warning message and put the malicious node's id and the current sequence number in the message. Then it broadcasts the message to the network. Each node receives the warning message; it modifies the stored sequence number of the source according to current sequence number in the warning message. Then, it deletes all paths that contain the sinkhole node's id from its route cache and adds this id to its black list. Hence, when a node receives a RREQ, it looks for the sender's id in its black list. If it can find the id in its black list, it will discard the RREQ. Otherwise, it processes the RREQ for routing discovery.

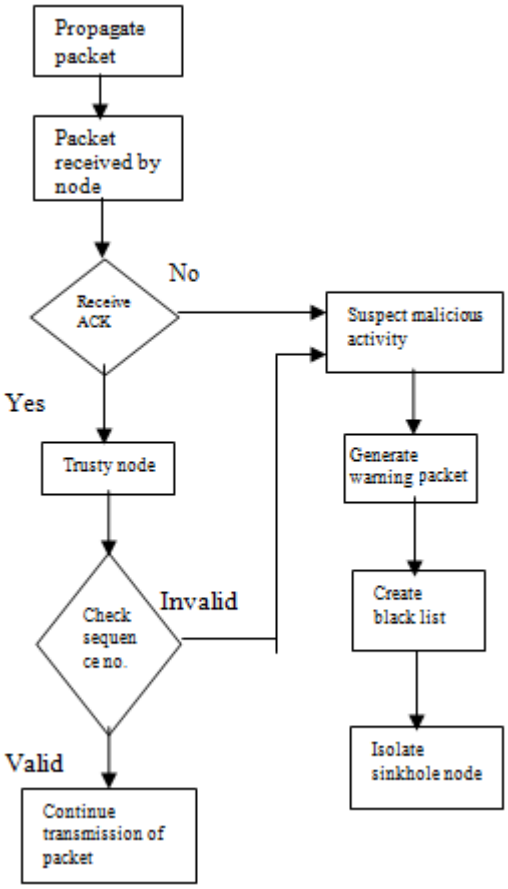

Figure: Flow Chart

References

[1] Mayank Gupta, Sachin Kumar, "Performance Evaluation of DSR, AODV And DSDV Routing protocol for Wireless Ad hoc Network", IEEE International Conference on Computational Intelligence & Communication Technology, pp. 417-421, 2015.
[2] Priya Malhotra, "Detecting Packet-Dropping Faults in Mobile Ad-Hoc Wireless Networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, pp. 558-561, February 2015.
[3] Sabarish D, Ranjani C, "Enhanced DSR Protocol for Detection and Exclusion of Selective Black Hole Attack in MANET", International Journal of Computer

Applications, vol. 112, pp. 32-35, February 2015.
[4] Nidhi N. Desai, Hiteishi Diwanji, J. S. Shah, "A Temporal Packet Marking Detection Scheme against MIRA Attack in MANET", IEEE Transaction, pp. 978-982, March 2014.
[5] Sunil Phulre, Pratima Gautam, Sadhna K. Mishra, "Implementation of Trusted Multitier method for Intrusion Detection in Mobile ad Hoc Networks with DSR Algorithm", Science and Information Conference London UK, pp. 666-673, August 2014.
[6] Mohammed Ashfaq Hussain, A. Francis Saviour Devaraj, "Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET", International Journal of Engineering Research and Applications, vol. 3, pp. 1737-1741, April 2013.
[7] Mohammad Rafiqul Alam, "Detecting Wormhole and Byzantine Attacks in Mobile ad hoc Networks" School of Electrical and Computer Engineering, May 2011.

Author Profile

Ms. Jeeja Borkar received the Bachelor of Engineering Degree in Computer Technology department and currently pursuing M.Tech. degree in Computer Science and Engineering from Kavikulguru Institute of Technology and Science, Ramtek from Rashtrasant Tukdoji Maharaj Nagpur university.

Ms. Vaishali Malekar assistant professor in Kavikulguru Institute of Technology and Science, Ramtek.