Enhanced DSR Protocol for Detection and Exclusion of Selective Black Hole Attack in MANET

Sabarish D,
PG Scholar, Department of CSE (PG)
Sri Ramakrishna Engineering College,
Coimbatore.

Ranjani C,
Assistant Professor, Department of CSE (PG),
Sri Ramakrishna Engineering College,
Coimbatore.

ABSTRACT
A Mobile Ad-hoc Network (MANET) is a collection of wireless nodes that can be dynamically set anywhere and anytime without using any pre-existing network infrastructure. MANET can operate without fixed infrastructure and can survive rapid changes in the network topology. The nodes in the network are free to move independently in any direction. The DSR protocol is modified to detect and isolate the selective black hole attack in MANETs. Secure Dynamic Source Routing Protocol (SDSR) is proposed 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) is proposed 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. When any anomaly is detected, the nearby IDS node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network. The SDSR is simulated using network simulator (NS2).

Keywords
Mobile ad hoc network, SDSR, selective black hole attack, IDS

1. INTRODUCTION
A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. A wireless network uses radio waves to connect devices such as laptops to the Internet and to business network and its applications. The development of wireless networks was motivated by military applications such as battlefield surveillance today such networks are used in many industrial and consumer applications such as industrial process monitoring and control machine health monitoring and so on. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad hoc is Latin and means "for this purpose". MANET is a self-configuring network of mobile routers (and associated hosts) connected by wireless links- the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily: thus, the network's wireless topology may change rapidly and unpredictably. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy. The characteristics of these networks are summarized as follows:

- Communication via wireless means.
- Nodes can perform the roles of both hosts and routers.
- No centralized controller and infrastructure.
- Intrinsic mutual trust.
- Dynamic network topology.
- Frequent routing updates.

1.1 Types of MANET
1 Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment.

2 Intelligent vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

3 Internet Based Mobile Ad hoc Networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly [13].

1.2 Routing in MANET
The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. The knowledge of routing protocols of MANETs is important to understand the security problems in MANETs [11,12,14]. The routing protocols used in MANETs are different from routing protocols of traditional wired world. Some of the reasons are listed below:

- Frequent Route updates.
- Mobility
- Limited transmission range

The performance criteria of nodes in MANETs are different than that of wired networks. Some of the performance metrics of MANET routing protocols are listed below:

- Route stability
- Control overhead
- Data rebroadcast overhead (for multicast)

1.3 Dynamic Source Routing
Dynamic source routing protocol (DSR) is an on-demand routing protocol. It is an on-demand protocol because routes are discovered at the time a Source sends a packet to the destination for which it has no cached route. DSR has two main functionalities: route discovery and route maintenance. It is designed to restrict the bandwidth consumed by control packet in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach [12, 14].

2. RELATED WORK
In [1], Santhosh kumar and suveg moudgil, proposes a reputation mechanism in DSR routing protocol, reputation of a node can be calculated using simple formula and a node is

supposed to maintain a good reputation value to participate in route discovery otherwise discard in route discovery. In a wireless mobile ad hoc network (MANET) [2], there are no basic network devices, such as routers or access points; data transfer among nodes is realized by means of multiple hops, and rather than just serving as a single terminal, every mobile node acts as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes.

A black hole attack on a MANET refers to an attack by a malicious node, which forcibly acquires the route from a source to a destination by the falsification of sequence number and hop count of the routing message [3]. A selective black hole is a node that can optionally and alternately perform a black hole attack or perform as a normal node. Several IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes must be set in sniff mode in order to perform the ABM (Anti-Black-hole Mechanism) function, which is mainly used to estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. When a suspicious value exceeds a threshold, an IDS nearby will broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node [4]. Due to the inherent vulnerabilities of wireless networks, new security measures need to be developed to efficiently safeguard them. This work focuses on the detection of malicious activities in MANETs. Proposed ideas for intrusion detection in these networks are required to achieve a trade-off between accurate detection and limited consumption of resources or the lack of central management and mobility of nodes.

The paper presents a comparison of different classification algorithms applied to detect intrusions in MANETs. These algorithms can help to discriminate ‘‘normal’’ against ‘‘intrusive’’ behavior effectively [5]. It uses six well-known classification algorithms, using labeled datasets obtained from a simulated environment. The comparison is fairly performed as several hyper-parameters were tuned and the experiments have been performed with datasets generated under various traffic conditions regarding the network mobility and the number of malicious nodes. Intrusion detection can be used as a mechanism for indicating possible security failures in the system. A simple way to perform intrusion detection is to use a classifier in order to decide whether some observed traffic data is ‘‘normal’’ or ‘‘abnormal’’. In the simplest case, the classification objective is to minimize the probability of error. However, in problems such as that of intrusion detection, authentication and fraud detection, the goal is not simply to predict the class with highest probability, but to actually take the decision with the lowest expected cost. For example, in intrusion detection, the cost of having an undetected attack is usually much more severe than triggering a false alarm. In cost-sensitive classification, decisions are made in order to minimize the expected cost, rather than the probability of error. The concept of cost-sensitive classification has been already investigated in wired networks.

An analysis of the impact of the proposed scheme shows that it allows a flexible approach to management of threats and demonstrates improved network performance with a low network overhead. The paper proposes a set of distributed algorithms that support an Intrusion Detection System (IDS) model for MANETs [6]. The development of mobile networks has implicated the need of new IDS models in order to deal with new security issues in these communication environments. More conventional models have difficulties to deal with malicious components in MANETs. The proposed IDS model focuses on distributed algorithms and their computational costs [7]. The proposal employs fault tolerance techniques and cryptographic mechanisms to detect and deal with malicious or faulty nodes. The model is analyzed along with related works. Unlike studies in the references, the proposed IDS model admits intrusions and malice in their own algorithms.

3. PROPOSED METHODOLGY

The basic approach of proposed protocol during the route discovery phase is to establish a route by flooding Route Request (RREQ) packets in the network. The destination node, on receiving a RREQ packet, responds by sending a Route Reply (RREP) packet back to the source by reversing the route information stored in the RREQ Packet. On receiving the RREQ, any intermediate node can send the RREP back to the source node if it has the route to reach the destination. During the Route maintenance phase, the link breaks are handled. A link break occurs when any intermediate node which involves in the packet forwarding process moves out of the transmission range of its upstream neighbor. If an upstream node detects a link break when forwarding a packet to the next node in the route path, it sends back a route error (RERR) message to the source informing it of that link break. The source either tries an alternate path available or initiates the route discovery process again.

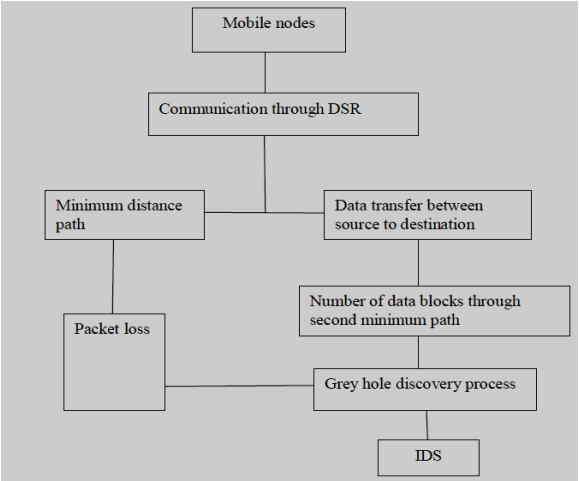

Fig 1 Architecture

Fig 1 is the architecture of secured DSR protocol. Mobiles nodes are connected in a network topology with n number of nodes. These nodes are communicated through DSR protocol by using intermediate nodes. The number of data blocks send from source node to destination node is received completely, and then the destination node will send a positive acknowledgement to the source node. If the destination node receives less number of packets, then it discovers a grey hole node in the network. The IDS will isolate the gray hole from the active path of the network.

When the source node has data packets to send to the destination, it divides the data to be transmitted into different blocks and sends one block of data at a time to the destination. It also intimates the number of data packets it sends in a block to the destination before the actual transmission of the data using a different route (2nd shortest path to reach destination). Let N_s denotes the number of blocks of data packets from source to destination and N_D be number of blocks received at destination. The probability of packets received at destination is

$$P_D = \frac{N_D}{N_S} \qquad 1$$

If P_D is less than the specified threshold value, then the destination node starts the grey hole discovery process [8].

3.1 Grey Hole Discovery Process

When the destination node discovers that the actual number of data packets it receives from its previous hop node is significantly less than the number of data packets the source node sends, it starts the grey hole node discovery processs [9]. When the destination node receives the QREP, it verifies the number of data packets it received from its previous hop node with that specified in the QREP. If it receives lesser number of packets from neighboring node than sender node, it assumes for grey hole attack and move to the next module called intrusion detection.

3.2 Intrusion Detection System (IDS)

Now the destination node intimates the suspected nodes in the source route to its nearby IDS nodes through an MNREQ (Malicious Node REQuest) packet. The MNREQ packet is forwarded to all the IDS nodes. The MNREQ packet is forwarded only by an IDS node to its neighbor IDS nodes and so on. After a periodic interval (for receiving MNREQ by all IDS nodes), the IDS node whose neighbor is the source node sends an ALARM packet to the source node to intimate the presence of attacker in the data forwarding path and ask them to send the next block of data. If any of the suspected nodes is found to be dropping data packets intentionally, it will be moved to the malicious node list. Then a block message is sent to all the nearby nodes by the IDS nodes which monitored them. Any IDS node that receives the block message will broadcast to its neighbors and hence the malicious node is isolated from the network. The block message is forwarded only by the IDS nodes to the network. Any normal node that receives the block message will learn the malicious node information and then drop the message without forwarding. Once the malicious node is located and isolated, all nodes remove any routing information involving the attacker node from their route cache and no future RREP involving the malicious node is considered [10,13].

4. EXPERIMENTAL SETUP AND ANALYSIS

This paper applies network simulator 2 (NS2) to validate the detection and exclusion efficiency of proposed method against selective black hole node.

4.1 Packet Drop Ratio

Ratio of the total number of data packets dropped by the malicious nodes and also due to congestion to the total number of data packets sent.

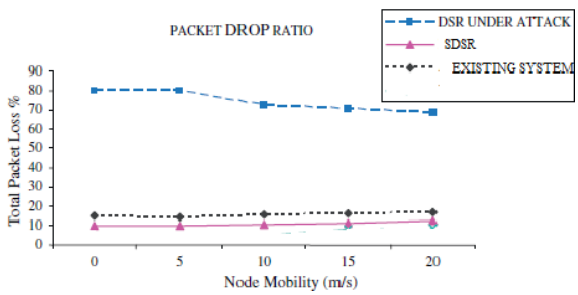

Fig 2 Packet drop ratio

The packet loss rate of DSR under attack was approximately 65%, while the packet loss rate of SDSR was approximately 11%, reduced by 54%. Similarly the packet loss rate of the existing system was approximately 15%, which was increased by 4% when compared to SDSR.

4.2 End to End Delay

It denotes the time elapsed between the moment of sending of a bit by the source node, and the moment of its reception by the destination node.

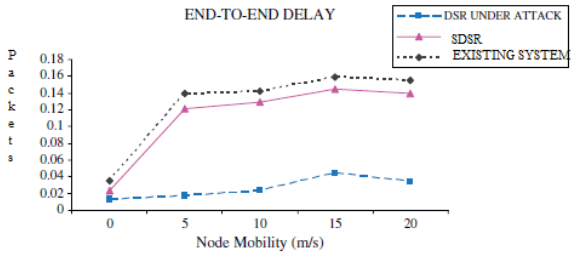

Fig 2 End to end delay

The end-to-end delay for sending data packets between the source and the destination is better in SDSR when compared to the existing system. This is because, the balck hole detection process is initiated only when malicious nodes are present in the source route, which is determined by verifying the number of data packets, received by the destination.

4.3 Packet delivery ratio

It denotes the total number of data packets delivered to destination from source node.

Fig 3 Packet delivery ratio

The packet delivery ratio is increased about 24 % when compared to the existing approach.

5. CONCLUSION AND FUTURE WORK

The secure DSR protocol is a light weight solution methodology which is a simple acknowledgement scheme to detect gray hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By the proposed algorithm, the destination node detects the presence of malicious nodes in the source route and with the help of intrusion detection system the malicious nodes are isolated from the network. The simulation results shows that the percentage of data packet loss in the proposed work is better than DSR in presence of multiple grey hole nodes. In the proposed algorithm, the destination node detects the presence of malicious node in the source route and with help of intrusion detection system, the malicious node are isolated from active path of the network. The future scope is to implement the methodology in other on-demand routing protocols and also to detect other attacks in MANETs.

6. REFERENCES

[1] Santhosh kumar and Suveg Moudgil, Detection of selfish node in DSR based MANET using reputation based mechanism, International journal of Research in IT, ISSN 2249-9482.

[2] Adnan Nadeem , Michael P. Howarth(2014)," An intrusion detection & adaptive response mechanism for MANETs", Ad Hoc Networks, vol 13, pp 368–380.

[3] Aikaterini Mitrokotsa , Christos Dimitrakakis(2013), "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection" Ad Hoc Networks, pg no 11, vol 226–237.

[4] Lacey T H, Mills R.F, Mullins B.E, Raines R.A, Oxley M.E, Rogers S.K.(2014)," RIPsec e Using reputation-based multilayer security toprotect MANETs" compute rs & security , 31122 e136.

[5] Mafraa P.M, Fragaa J.S , Santin A.O(2014), "Algorithms for a distributed IDS in MANETs", Journal of Computer and System Sciences, pp 80, vol 554–570.

[6] Manickam, T. Guru Baskar , M.Girija, Dr.D.Manimegalai(2001), 'Performance comparison of routing protocols in mobile ad-hoc networks' International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1.

[7] Ming-Yang Su(2011)," Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications ,pp 34, vol 107–117.

[8] Mohanapriya. M, Ilango Krishnamurthi(2014)," Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering, vol 40, pp530–538.

[9] Yih-Chun Hu, Adrian Perrig, David B. Johnson IEEE,Wormhole Attacks in Wireless Networks, vol 13(6), pp24–30.

[10] Sergio Pastrana a, Aikaterini Mitrokotsa , Agustin Orfila , Pedro Peris-Lopez (2012)," Evaluation of classification algorithms for intrusion detection in MANETs", Knowledge-Based Systems, vol 36, pp217–225.

[11] Abolhasan Mehran, Wysocki Tadeuz. A review of routing protocols for mobile ad hoc networks. Int J Ad hoc Networks 2004;2(1):1–22.

[12] Johnson DB, Maltz DA, Hu Y-C. The dynamic source routing protocol for mobile ad-hoc network (DSR). IETF Internet Draft 2004.

[13] Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput Commun 2010.

[14] Anit kumar, Pardeep Mittal, A comparative study of AODV and DSR routing protocols in Mobile ad-hoc networks, ijarcsse, Volume 3, Issue 5, May 2013, ISSN: 2277 128X .

[15] Neha Shrivastava, Anand Motwani, Survey of malicious attacks in MANET, International Journal of Computer Applications (0975 – 8887), Volume 80 – No 14, October 2013.