Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Efficient Detection and Prevention of Jamming Attack in MANETs

Ashwinder Kaur
Dept of Computer Science Engg.,
Mtech Full Time
RIMT IET, Punjab India

Abhilash Sharma
Assistant Professor
Dept of CSE
RIMT IET, Punjab, India

Abstract: MANET the branch of networking that deals with mobile ad-hoc networks. This network deals with mobility of nodes throughout the communication. These nodes communicate with each other without and interference communication. Various attacks have been introduced in MANET that affect the performance of the network. In this paper various attacks and their affects on the network have been studied. In this paper the approaches have been purposed that can reduce the affect of attacks occurred in the MANET environment. In this paper approach that has been purposed can be used to control the jamming attack occur in the network.

Keyword: MANET, DOS, DSDV, AODV and DSR

I. INTRODUCTION

1.1MANET: A MANET is a kind of specially appointed system that can change areas and design itself on the fly. Since MANETS are portable, they utilize remote associations with join with different systems. This can be a standard Wi-Fi association, or an alternate medium, for example, a cell or satellite transmission. A few MANETs are confined to neighbourhood remote gadgets; others may be joined with the Internet. Case in point, A VANET (Vehicular Ad Hoc Network), is a kind of MANET that permits vehicles to speak with roadside gear. While the vehicles might not have a direct Internet association, the remote roadside gear may be joined with the Internet, permitting information from the vehicles to be sent over the Internet. The vehicle information may be utilized to gauge movement conditions or stay informed regarding trucking armadas. As a result of the element way of MANETs, they are regularly not extremely secure, so it is critical to be careful what information is sent over a MANET.

1.2 ATTACKS IN MANET

1.2.1 Passive attack: In this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

1.2.2 Denial of service attack: Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

1.2.3 Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries.

1.2.4 Snooping: Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

1.2.5 Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed

1.2.6 Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial – of -service.

1.2.7 Black hole Attack: Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

1.2.8 Jamming: Jamming is a special class of DOS attacks which are initiated by malicious node after determining the frequency of communication in this type of attack; the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

1.2.9 Active Interference: An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information.

1.2.10 Selfish Misbehavior of Nodes: Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network. It may include two important factors.

1.2.11 Sleep Deprivation: In sleep deprivation attack, the resources of the specific node/nodes of the network are consumed by constantly keeping them engaged in routing decisions. The attacker node continually requests for either existing or non-existing destinations, forcing the neighboring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.

1.2.12 Node Isolation Attack: The authors in this work have introduced an attack against the OLSR protocol. As implied by the name, the goal of this attack is to isolate a given node from communicating with other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

1.2.13 Routing Table Poisoning Attack: Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number. This causes all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

1.2.14 Blackmail: The attack incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

1.2.15 Snare Attack: Lin et al. have proposed the snare attack, which relates to military specific applications. In a battlefield, a node could be physically compromised (say when the corresponding soldier is caught by the enemy). Afterwards, the compromised node could be used to lure a Very Important Node, (say the commander), into communicating with it. Since the adversary can easily intercept any transmission in the network through the compromised node, the adversary can identify the physical location of the VIN by tracing and analyzing some routes. After locating the VINs, the adversary will be able to launch a Decapitation Strike on those VINs as a short cut to win the battle.

1.3 Applications of MANET:

1.3.1 Military Battlefield: Military equipment now routinely contains some sort of computer\ equipment. Ad-hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

1.3.2 Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

1.3.3 Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

1.3.4 Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context

II. RELATED WORK

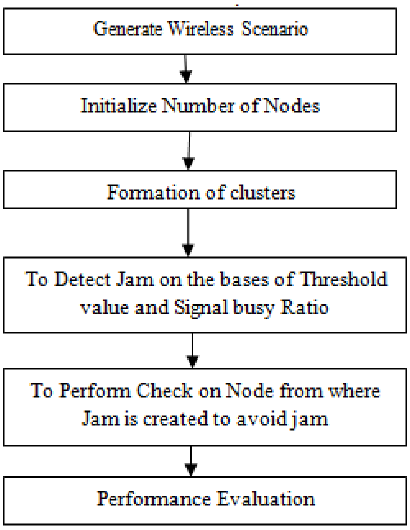
Aleksi Marttinen et al [1] "Statistics-based Jamming Detection Algorithm for Jamming Attacks Against Tactical MANETs" In this paper, we propose an identification approach for receptive sticking assaults in the strategic remote specially appointed systems. A noteworthy soft spot for all remote correspondence frameworks is a weakness to sticking assaults. In the most dire outcome imaginable, jammers have the possibility to totally square information transmissions in the remote system. Since strategic systems are regularly used in emergency administration and war zone operations, dependable and secure interchanges is a basic component for mission achievement. In this way, sticking assaults must be identified and alleviated quickly by the remote system. New methodologies for the discovery and relief of sticking assaults are needed, particularly for strategic systems in light of portable specially appointed innovation where brought together identification calculations are unusable. We show a novel component to recognize sticking in strategic specially appointed systems, which is in view of the obliged number of re-transmission endeavors of transmitted bundles and parcel conveyance rate of got parcels. Our proposed methodology utilizes a few system execution parameters, which separates our methodology from most existing location calculations, since just a solitary parameter is usually utilized as a recognition choice. The reproduction model of proposed discovery calculation is executed in ns-3 system test system.

Akshai Aggarwal et al [2] "PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS" Portable Ad hoc Networks (MANETs) are considered as another standard of foundation less versatile remote correspondence frameworks. MANETs are as a rule broadly mulled over and it is the innovation that is pulling in a huge mixture of uses. Directing in MANETs is viewed as a testing assignment because of the unusual changes in the system topology, coming about because of the arbitrary and incessant development of the hubs and because of the unlucky deficiency of any unified control. In this paper, we assess the execution of receptive steering conventions, Ad hoc On interest Distance Vector (AODV) and Dynamic Source Routing (DSR) and proactive directing convention Destination Sequenced Distance Vector (DSDV).The real objective of this study is to break down the execution of surely understood MANETs steering convention in high versatility case under low, medium and high thickness situation. Not at all like military applications, the vast majority of alternate uses of MANETs oblige moderate to high versatility. Consequently it gets to be imperative to consider the effect of high portability on the execution of these steering conventions. The execution is broke down as for Average End-to-End Delay, Normalized Routing Load (NRL), Packet Delivery Fraction (PDF) and Throughput. Reproduction results confirm that AODV gives better execution when contrasted with DSR and DSDV.

V. Rajeshkumar et al [3] "Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2" Mobile Ad hoc Network (MANET) is an accumulation of remote versatile hubs that alertly frame a system briefly with no backing of focal administration. In addition, Every hub in MANET moves self-assertively making the multi-bounce system topology to change haphazardly at unverifiable times. There are a few well known directing conventions like AODV, DSR, and DSDV and so on… which have been proposed for giving correspondence among every one of the hubs in the remote system. This paper shows an execution examination and investigation of receptive and proactive conventions AODV, DSR and DSDV in view of measurements, for example, throughput, control overhead, parcel conveyance proportion and normal end-to-end defer by utilizing the NS-2 test system.

Sachin Kumar Gupta et al [4] "PERFORMANCE METRIC COMPARISON OF AODV AND DSDV ROUTING PROTOCOLS IN MANETs USING NS-2" Productive directing conventions can give huge advantages to portable specially appointed systems as far as both execution and unwavering quality. Versatile Ad-hoc Network (MANET) is a base less and decentralized system which require a hearty element directing convention. Numerous directing conventions for such systems have been proposed in this way. Amongst the most prominent ones are Dynamic Source Routing (DSR), Ad-hoc On-interest Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA) and Destination-Sequenced Distance Vector (DSDV) steering convention. The execution of AODV and DSDV steering convention have been assessed for Mobile Ad-hoc Networks (MANETs) as far as throughput, the normal end to end defer, jitter and drop and so on. The execution of the AODV is superior to the execution of the DSDV steering convention. A system test system 2 (NS-2) called Mobile REAL test system has been planned and created for execution assessment of AODV and DSDV steering convention in this paper. To look at the execution of AODV and DSDV steering convention, the reproduction results were dissected by graphical way and follow document in light of Quality of Service (QoS) measurements, for example, throughput, drop, deferral and jitter. At long last, the execution differentials taking into account system load, portability, and system size have been broke down. The reenactment result examination confirms the DSDV and AODV steering convention exhibitions.

III. METHODOLOGY


Generate Wireless Scenario
Initialize Number of Nodes
Formation of clusters
To Detect Jam on the bases of Threshold value and Signal busy Ratio
To Perform Check on Node from where Jam is created to avoid jam
Performance Evaluation

First of all generate the wireless scenario. Then Initialize the number of nodes. Cluster formation will be achieved and then jam will be detected on the bases of threshold and signal busy ratio. When the jam will detected then check will be performed on the node which will be creating jam. Node identity will be checked by calculating the distance and the message of that node will be checked to detect the retransmission and replays. If sequence number will same than attacker will be detected but if sequence number is different message content will be checked. To check the reason of retransmissions an additional message will be send to destination so that if re-transmissions are due to the network failure it can be detected.

IV. ALGORITHM USED

DSDV: Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for networks based on the Bellman–Ford algorithm. It was developed by C. Perkins and P. Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently.

AODV (AD-HOC ON-DEMAND DISTANCE VECTOR): The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed (a packet is ready to be sent) until the time the route is actually acquired. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection.

V. CONCLUSION

MANET is the wireless network that is used for communication between different devices without interference of any outer source. In this network each node can communication with other through wireless channel. In this paper different attacks have been studied. These attacks can be reduced by using different approaches. In this paper the jamming attack is resolved by using threshold based approach that optimizes the network signal by sensing the channel. This purposed work can be simulated for performance analysis over various previous approaches and can be used in real world applications.

REFRENCES

[1] Aleksi Marttinen "Statistics-based Jamming Detection Algorithm for Jamming Attacks against Tactical MANETs", *IEEE Conference on Communications and Network Security (CNS), 2014,* pp. 14 – 20.

[2] Akshai Aggarwal "PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS" *International Conference on Advances in Engineering and Technology Research (ICAETR), 2014*, pp. 1 – 5.

[3] V. RAJESHKUMAR "Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2" *Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012, pp.* 114 – 121.

[4] Sachin Kumar Gupta **et al [5]** "PERFORMANCE METRIC COMPARISON OF AODV AND DSDV ROUTING PROTOCOLS IN MANETs USING NS-2" *International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2014,* pp. 1 – 7.

[5] Hongwei Li "A Hierarchical Identity-Based Encryption for MANETs" *International Conference on Computational Problem-Solving (ICCP), 2011*, pp. 330 – 333.

[6] Ahmad, S.J., Reddy, V.S.K. , "Efficient path estimation routing protocol for QOS in long distance MANETs", pp. 178 – 183.

[7] Benchi, A., "JOMS: A Java Message Service Provider for Disconnected MANETs" *26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2012*, pp. 484 – 489.