Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Jamming Attack in MANETS and its Various Approaches

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

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

Abstract- In wireless network jamming attack is main problem and this can affect the network by various ways. Sometimes jammer retransmits messages to create jam over network or sometimes jammers are radio jammer which disturbs communication by decreasing the signal to noise ratio. Jamming can also be arise because of various different reasons like it can be intentionally created by attackers which lead to denial of service attack or it can be unintentionally created on network due to congestion. In previous researches various techniques are discussed to detect jamming. One way is to check the signal busy ratio. If channel is busy for long time that means there is a jam on network or it can be check by checking the threshold value. If threshold value exceeds up to some limit then there expect some jam on network. But there is still some work can be done. This attack can be prevented by blacklisting the nodes. It can be possible by applying check on nodes.

Keyword: MANET, Various Attacks, Jamming Attack.

I. INTRODUCTION

1.1 MANET

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 neighborhood 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 ISSUES IN MANET'S

Design and analysis of routing protocols are the key issues in MANET. The essential objective of a MANET directing convention is to create a right and efficient course between a couple of two hosts for conveying message in an auspicious way. Numerous different directing conventions have been proposed for MANETs. They can be classified into two classifications: table-determined and on-interest.

The table-driven steering conventions are like and come as a characteristic expansion of those for the wired systems including Internet. They basically utilize proactive plans, which endeavor to keep up predictable cutting-edge directing data from each one host to each other hub in the MANET. These conventions require each one host to keep up one or more tables to contain most recent steering data, and any change in system topology needs to be reflected by TV redesigns data all through the system with a specific end goal to keep up a predictable system view. Then again, the on-interest steering conventions take a languid methodology to directing. The inspiration behind the on-interest conventions is to lessen vast measure of overhead for keeping up the steering table in the table-driven conventions in the element MANET. They are source-launched plans which don't keep up alternately always overhaul their course tables with the most recent course topology. This kind of directing makes courses just when wanted by the source hub. At the point when a hub obliges a course to a terminus, it starts a course revelation transform inside the system. This methodology is finished once one or more courses are discovered or all conceivable course stages have been analyzed. Nonetheless, steering overhead for on-interest conventions might be still substantial for the most part in light of the fact that the flooding methodology utilized as a part of finding courses, where the source (i.e., the host looking for a course) floods the whole system with an inquiry parcel in looking a course to the terminus.

1.3 ATTACKS IN MANET

Securing remote impromptu systems is an exceedingly difficult issue. Understanding conceivable type of assaults is dependably the first step towards creating great security arrangements. Security of correspondence in MANET is vital for secure transmission of information. Absence of any focal co-appointment system and imparted remote medium makes

MANET more defenseless against advanced/digital assaults than wired system there are a number of assaults that influence MANET. These assaults can be characterized into two sorts:

- **External Attack:** Outer assaults are done by hubs that don't have a place with the system. It causes blockage sends false steering data or reasons inaccessibility of administrations.
- **Internal Attack:** Inward assaults are from bargained hubs that are a piece of the system.In an inward assault the noxious hub from the system increases unapproved access and mimics as a veritable hub. It can investigate activity between different hubs and may take an interest in other system exercises.

1.4 SECURITY IN MANET

A considerable measure of exploration has been carried out in the past however the most huge commitments have been the PGP (Pretty Good Privacy) and trust based security. None of the conventions have made a respectable exchange off in the middle of security and execution. While trying to improve security in MANETs numerous analysts have proposed and executed new enhancements to the conventions and some of them have recommended new conventions.

II. LITERATURE SURVEY

Aleksi Marttinen et al [1] "Measurements based Jamming Detection Algorithm for Jamming Attacks against Tactical MANETs" In this paper, Author was proposed a discovery approach for receptive sticking assaults in the strategic remote impromptu systems. A noteworthy soft spot for all remote correspondence frameworks is powerlessness to sticking assaults. In the direst outcome imaginable, jammers have the possibility to totally square information transmissions in the remote system. Since strategic systems are commonly used in emergency administration and front line operations, dependable and secure interchanges are a basic variable for mission achievement. Along these lines, sticking assaults must be identified and relieved instantly by the remote system. New methodologies for the discovery and relief of sticking assaults are needed, particularly for strategic systems in view of versatile impromptu innovation where incorporated recognition calculations are unusable. We introduce a novel instrument to distinguish sticking in strategic impromptu 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 identification calculations, since just a solitary parameter is generally utilized as a recognition choice. The reenactment model of proposed location calculation is actualized in ns-3 system test system.

Marttinen, A. et [2] "Moving-target safeguard components against source-particular sticking assaults in strategic cognitive radio MANETs" In this paper, we propose procedures for fighting source specific sticking assaults in strategic cognitive MANETs. Secure, solid and consistent interchanges are essential for encouraging strategic operations. Particular sticking assaults represent a genuine security danger to the operations of remote strategic MANETs since specific procedures have the possibility to totally detach a share of the system from different hubs without giving an acceptable sign of an issue. Our proposed alleviation systems utilize the idea of location control, which vary from different methods displayed in open writing following our strategies utilize de-focal construction modeling as opposed to an unified system and our proposed procedures don't require any additional overhead. Trial results demonstrate that the proposed procedures empower correspondences in the vicinity of source particular sticking assaults. At the point when the vicinity of a source particular jammer pieces transmissions totally, executing a proposed flipped location system expands the normal number of obliged transmission endeavors just by one in such situation. The likelihood that our second approach, irregular location task, neglects to tackle the right source MAC location can be as little as 10-7 when utilizing exact parameter choice.

Sharma, P. et al [3] "Improved security plan against Jamming assault in Mobile Ad hoc Network" Security is the one of the significant concerns in Mobile Ad hoc Network (MANET). Because of its interesting foundation, it makes various considerable difficulties to the security outline. There is a need to make a conventional tradeoff in the middle of security and execution. In versatile impromptu systems where the system topology animatedly changes customary security routines can't be connected proficiently. Distinctive security plans against assault enhances the execution of system even in the vicinity of assailant and tries to incapacitate trouble making movement. In this paper we have proposed an improved security plan against sticking assault with AOMDV directing convention. The sticking assailant conveys colossal measure of unapproved bundles in the system and thus system gets congested. The proposed plan recognizes the sticking assailant and hinders its exercises by recognizing the tainted or unapproved parcels in system. Multipath steering convention AOMDV is utilized to enhance the system execution however there is a condition that sticking stage happens regularly and is not attained to by assailant deliberately. In vicinity of assailant security conspire dependably gives the protected way and through multipath steering the likelihood of secure directing is upgraded. Reenactment results and PDR (Packet Delivery Ratio) estimations of every hub obviously shows better system execution if there should arise an occurrence of security plan in vicinity of Jamming assault.

Arora, D. et al [4] "Sticking Strategies in DYMO MANETs: Assessing Detectability and Operational Impacts" The wide sending of advanced mobile phones has started to make them realistic organization situations for true at-scale MANETs (i.e., to give shared based non-cell administrations). Such administrations, obviously, will be liable to digital assaults, one of the most straightforward of which is radio recurrence (RF) sticking. The accomplishment of these MANETs will require both: i) vigorous and precise techniques for recognizing when jammers are available and ii) strategies for relieving jammer sways. This work investigates the impacts that different jamming strategies have on MANET operations as watched by means of standard MANET operational measures, for example, bundle conveyance proportion, deferral, directing overhead, and bounces voyaged. It is demonstrated that the identify capacity of dynamic jammers intensely depends both on which measure is utilized and the definite way of the jamming strategy utilized. Additionally, albeit fundamental methodologies, for example, steady sticking are effectively noticeable, it is demonstrated that little work is obliged to develop far less discernible sticking methods.

Throat, S.A. et al [5] "Design issues in trust based guiding for MANET" In MANET center points help each other in data coordinating. MANET works outstandingly if the sharing centers coordinate with each other. It is preposterous to expect that, all centers joining in an open MANET are satisfactory and authentic. For individual center points it may be beneficial to be non-satisfactory and selfish. However non-cooperation, selfishness and dangerous behavior of the sharing center points may happen into breakdown of a MANET. Trust based coordinating computations plan to perceive misbehaving and non-arranging center points in the MANET. These computations enhance the framework execution by utilizing tried and true center points as a part of convincing way and rebuffing non-supportive centers. This paper takes a gander at trust based and cryptographic procedures for realizing security in MANET directing. The paper inspects blueprint issues in trust based controlling traditions for MANET in purposes of investment. The paper demonstrates a review on trust based controlling traditions for MANET. The paper offers course to future research in trust based directing for MANET.

Hongwei Li [6] "A Hierarchical Identity-Based Encryption for MANETs" Mobile impromptu systems (MANETs) have no settled base, for example, base stations or versatile exchanging focuses, and the structure is dynamic owing to successive changes in both topology and participation. Subsequently, the trust connections among hubs additionally change, and numerous security arrangements with static designs will get to be insufficient. Security in MANETs keeps on pulling in consideration following quite a while of examination. Late advances in personality based cryptography (IBC) reveals insight into this issue and have gotten to be prominent as an answer base. Taking into account whole number grids, we first present a novel Hierarchical Identity-Based Model for MANETs (HIBMM). At that point, we propose a Hierarchical Identity-Based Encryption for MANETs (HIBEM). HIBEM accomplishes security under the grid hard issue. At last we investigate the rightness and security.

III. APPROACHES USED

DSR (Dynamic Source Routing):

The Dynamic Source Routing (DSR) convention is one of the all the more for the most part acknowledged on demand directing conventions. It is common to consider the DSR convention with multiple courses since they might be manufactured amid the course disclosure by flooding. The Dynamic Source Routing (DSR) convention proposed additionally has a choice of keeping up various courses, so a substitute course can be utilized upon disappointment of the essential one. Be that as it may in DSR an excess of courses are kept up in an unimportant way, without any respect to their definitive helpfulness. Dynamic Source Routing (**DSR**) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

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. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

Approach Used	Advantages	Disadvantages
DSR	This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in	The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link

	a table-driven approach. In a reactive (on-demand) approach	
AODV	The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination.	The Disadvantage of AODV is unnecessary bandwidth consumption due to periodic beaconing.

IV. CONCLUSION

Akshai Aggarwal [9]

Parameters	Protocols	Performance		
		Low	Moderate	High
Delay	AODV	Low		
	DSR		Mod	
	DSDV			High
Load	AODV	Low		
	DSR			High
	DSDV		Mod	
Packet Delivery Ratio	AODV			High
	DSR		Mod	
	DSDV	Low		
Throughput	AODV			High
	DSR		Mod	
	DSDV	Low		

V. RajeshKumar[10]

Parameters	Protocols	Performance		
		Low	Moderate	High
Packet Delivery Ratio	AODV		Mod	
	DSR			High
	DSDV	Low		
Control Overhead	AODV		Mod	
	DSR			High
	DSDV	Low		
Throughput	AODV			High
	DSR		Mod	
	DSDV	Low		
Delay	AODV	Low		
	DSR		Mod	
	DSDV			High

Sachin kumar [11]

Parameters	Protocols	Performance	
		Low	High
Throughput	AODV	Low	
	DSDV		High
Delay	AODV		High
	DSDV	Low	
Jitter	AODV	Low	
	DSDV		High

From above study it is analyzed that results depends upon the scenario parameters like number of nodes, Channel Used, Protocols used etc. It has been analyzed that among these three protocols **AODV** gives better performance as compared to DSR & DSDV.

REFRENCES

[1] Aleksi Marttinen, Riku Jantti, Alexander M. Wyglinski “Statistics-based Jamming Detection Algorithm for Jamming Attacks Against Tactical MANETs” IEEE Military Communications Conference, 2014,pp. 501-506.

[2] Martine, A.,Wyglinski, A.M., Jantti, R. “Moving-target defense mechanisms against source-selective jamming attacks in tactical cognitive radio MANETs” IEEE Conference onCommunications and Network Security (CNS), 2014,pp. 14 – 20.

[3] Sharma, P., “Enhanced security scheme against Jamming attack in Mobile Ad hoc Network” International Conference on Advances in Engineering and Technology Research (ICAETR), 2014,pp. 1 – 5.

[4] Arora, D., “Jamming Strategies in DYMO MANETs: Assessing Detectability and Operational Impacts” Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012,pp. 114 – 121.

[5] Thorat, S.A., “Design issues in trust based routing for MANET” International Conference onComputing, Communication and Networking Technologies (ICCCNT), 2014,pp. 1 – 7.

[6] Hongwei Li “A Hierarchical Identity-Based Encryption for MANETs” International Conference onComputational Problem-Solving (ICCP), 2011,pp. 330 – 333.

[7] Ahmad, S.J., Reddy, V.S.K. , “Efficient path estimation routing protocol for QoS in long distance MANETs”.178 – 183.

[8] Benchi, A., “JOMS: A Java Message Service Provider for Disconnected MANETs” 26th International Conference onAdvanced Information Networking and Applications Workshops (WAINA), 2012,pp. 484 – 489.

[9] Akshai Aggarwal “PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS” , International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011.

[10] V. RAJESHKUMAR “Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013.

[11] Sachin kumar “performance metric comparison of AODV and DSDV routing protocols in MANETS using ns-2”, ijrras 7 june 2011